October 15, 2003

Acquisition

Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems

(D-2004-008)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

C4I	Command, Control, Communications, Computers, and Intelligence
CRD	Capstone Requirements Document
DITSCAP	DoD Information Technology Security Certification Accreditation Program
GIG	Global Information Grid
IA	Information Assurance
JITC	Joint Interoperability Test Command
NS	National Security
ORD	Operational Requirements Document
SEP	System Evaluation Plan
SER	System Evaluation Report
SSAA	System Security Authorization Agreement
TEMP	Test and Evaluation Master Plan
TRADOC	Army Training and Doctrine Command

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

October 15, 2003

MEMORANDUM FOR AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Report on the Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems (Report No. D-2004-008)

We are providing this report for review and comment. This report is the second in a series of reports that discuss the implementation of interoperability and information assurance policies for the acquisition of DoD systems. This report addresses the implementation of those policies within the Army. In preparing the final report, we considered comments from the Director, Operational Test and Evaluation; the Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology); and the Office of the Army Chief Information Officer. However, the Army Deputy Chief of Staff for Operations and Plans did not respond to the draft report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. With the exception of clarifying that the interoperability certification is a requirement, management comments on the draft of this report conformed to the requirements of the Directive. Therefore, in response to the final report, we request that the Office of the Army Chief Information Officer clarify its comments on obtaining interoperability certification on an exception basis and that the Army Deputy Chief of Staff for Operations and Plans comment on this report by December 15, 2003.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to Aud-am@dodig.osd.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. John E. Meling at (703) 604-9091 (DSN 664-9091) or Mr. Jack D. Snider at (703) 604-9087 (DSN 664-9087). See Appendix G for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Mary L. Ugone
Acting Director
Acquisition Management Directorate

Office of the Inspector General of the Department of Defense

Report No. D-2004-008 **October 15, 2003**
(Project No. D2002AE-0187)

Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems

Executive Summary

Who Should Read This Report and Why? Civil Service and military managers, who are responsible for interoperability and information assurance requirements of Army weapon systems, should be interested in this report. This report addresses the importance of adhering to DoD and Army interoperability and information assurance policies to reduce the risk of Army weapon systems not being interoperable and able to exchange information in a secure manner with other DoD and allied systems.

Background. This report is the second in a series of reports on the implementation of interoperability and information assurance policies for the acquisition of DoD weapon systems. This report addresses the implementation of those policies within the Army. The first report addressed the implementation of those policies within the Office of the Secretary of Defense and the Defense agencies. Other reports in the series will address how effectively the Navy and the Air Force implement those policies and the impact of the Military Departments' implementation at the unified combatant commands. Interoperability and information assurance policies include the Joint Vision 2020 and the Global Information Grid capstone requirement document.

Results. The Army did not implement DoD policy that required the Army to define how each Army system will interface within the Global Information Grid to achieve joint interoperability, did not adequately address interoperability during the requirements generation process, and did not consistently conduct information assurance testing for Army acquisition programs. As a result, the Army has not ensured that 33 of 41 systems reviewed have the most effective, efficient, and assured information-handling capabilities available, consistent with national military strategy, operational requirements, and best-value enterprise-level business practices. Issuing and implementing guidance to define how each Army system will interface within the Global Information Grid; identifying interoperability and supportability requirements and developing testable information assurance requirements during the requirements generation process; identifying roles and responsibilities of combat developers in the DoD Information Technology Security Certification and Accreditation Process; and requiring the system security authorization agreement signatories to coordinate with the Army Test and Evaluation Command throughout the acquisition cycle for Army systems subject to the DoD Information Technology Security Certification and Accreditation Process should bring the oversight and improvements needed to those issues. (See the Finding section of the report for the detailed recommendations.)

Management Comments and Audit Response. We received comments from the Director, Operational Test and Evaluation; the Principal Director for Enterprise Integration, Office of the Army Chief Information Officer; and the Acting Deputy for Systems Management, Office of the Assistant Secretary of the Army (Acquisition,

Logistics, and Technology); however, we did not receive comments from the Army Deputy Chief of Staff for Operations and Plans on the draft report. The Director, Operational Test and Evaluation agreed with the findings and recommendations. The Principal Director, responding for the Secretary of the Army and the Army Chief Information Officer, concurred with recommendations to issue and implement guidance to comply with Global Information Grid (GIG) policy, to expedite efforts to populate and maintain the Army's portion of the GIG asset inventory, to provide Army combat developers with training on the GIG, to update Army acquisition and materiel requirements policy, and to validate warfighting requirements. However, the Principal Director stated that program managers should not obtain interoperability certifications, except by exception. The Acting Deputy for Systems Management concurred with the recommendations to update Army acquisition policy concerning testable information assurance requirements, roles and responsibilities of combat developers, and test and evaluation coordination. Further, although not required, the Principal Director commented on recommendations addressed by the Acting Deputy. (See the Finding section of this report for a discussion of the management comments and the Management Comments section of the report for the complete text of the comments.)

Office of the Secretary of Defense guidance requires program managers to obtain interoperability certifications. Therefore, we request that the Principal Director clarify his response on program managers obtaining interoperability certifications on an exception basis. Further, we request that the Army Deputy Chief of Staff for Operations and Plans provide comments on the recommendation to update Army acquisition and materiel requirements policy. The comments on this report should be provided by December 15, 2003.

Table of Contents

Executive Summary i

Background 1

Objectives 3

Findings

A. Compliance With the Global Information Grid 4
B. Implementing Interoperability Policies 10
C. Information Assurance Testing of Army Systems 20

Appendixes

A. Scope and Methodology 33
Prior Coverage 34
B. Glossary 35
C. Global Information Grid 43
D. Army Interoperability and Information Assurance Survey Results 45
E. Army Programs Surveyed 51
F. Information Assurance Requirements Policy 52
G. Report Distribution 54

Management Comments

Director, Operational Test and Evaluation 57
Secretary of the Army and Army Chief Information Officer 58
Assistant Secretary of the Army (Acquisition, Logistics, and Technology) 65

Background

This report is the second in a series of reports on the implementation of interoperability and information assurance (IA) policies within DoD. This report addresses the Army's implementation of those policies in the:

- interoperability requirements generation process and the oversight thereof;
- inclusion of adequate interoperability key performance parameters in the requirements documents; and
- interoperability certification process for Army systems.

Appendix B provides a glossary of technical terms used in this report.

Chairman of the Joint Chiefs of Staff Testimony on the President's Proposed Defense Program for FYs 2003 to 2007. On February 6, 2002, General Myers, the Chairman of the Joint Chiefs of Staff, testified before the U.S. House of Representatives Committee on Armed Services. General Myers described how Army, Navy, Air Force, and Marine Corps systems shared information to execute combat operations in Afghanistan. He testified that:

> To fulfill our range of commitments and protect our global interests, we must make the investments necessary to maintain the quality of our force, while preparing for future challenges of the 21st [century.] The best means of accomplishing these goals are to improve our joint war-fighting capability, and transform the armed forces into a 21st century force.

Quadrennial Defense Review. On September 2001, the Quadrennial Defense Review report stated that achieving the objectives of the defense strategy requires the transformation of the U.S. Armed Forces. Two of the six critical operational goals for the DoD transformational efforts relate to IA and interoperability:

- assuring that, in the face of attack, information systems conduct effective information operations; and
- leveraging information technology and innovative concepts to develop interoperable, joint command, control, communications, computers, intelligence, surveillance, and reconnaissance architectures and capability that includes an adaptable joint operational picture.

Joint Vision 2020. On May 30, 2000, the Chairman of the Joint Chiefs of Staff issued Joint Vision 2020, which addressed the concept to design, and produce systems with joint warfighting requirements. Joint Vision 2020 describes in broad terms a future joint force whose operational capabilities will be required to succeed across the full range of military operations and accomplish missions in the year 2020 and beyond. Joint Vision 2020 states that interoperability is a mandate for the future joint force especially for communications, common logistics items, and information sharing. Information systems and equipment that enable a

common, relevant operational picture must work from shared networks that can be accessed by any appropriately cleared participant. Another tenet of Joint Vision 2020 is to attain information superiority. Information superiority supports providing the right information to the right people, at the right time, and in the right format, resulting in a vastly improved shared understanding of the situation.

Global Information Grid. In November 1999, the Joint Chiefs of Staff assigned the Commander, U.S. Joint Forces Command the task of preparing the capstone requirements document (CRD) for the Global Information Grid (GIG). On August 30, 2001, the Joint Requirements Oversight Council approved the CRD, which describes the overarching information capability requirements for a globally interconnected, end-to-end, interoperable, and secured system-of-systems that would support the Secretary of Defense, the warfighter, DoD personnel, the intelligence community, policy makers, and non-DoD users at all levels involved in military and nonmilitary operations. Appendix C discusses the GIG.

Army Transformation Roadmap. The Army Transformation Roadmap details how the Army plans to progress towards attaining the goals for transformation outlined in the FY 2001 Quadrennial Defense Review. To meet three of the DoD transformation pillars of strengthening joint operations, experimenting with approaches to warfare and operational capabilities, and leveraging intelligence and information technology, the Army will:

- work directly with the Joint Staff, the Joint Forces Command, and the Office of the Secretary of Defense's Office of Net Assessment;
- evaluate concepts and technology in Joint and Army experimentation by leveraging laboratories, analysis, and experimentation plans supporting the development of the Objective Force; and
- ensure reciprocity with the Joint Force's entire range of capabilities by embedding full interoperability in its command, control, communications, computers, intelligence (C4I), surveillance, and reconnaissance technology.

The Army plans to achieve integration by incorporating compatible technologies and by standardizing interfaces and components across the force using experiments and training. Furthermore, the Army plans to develop a mobile and flexible wireless infrastructure for passing secure and non-secure voice, data, and video to ground commanders. This infrastructure constitutes the Army's contribution to the GIG.

Concepts to Develop a Secure Interoperable Joint C4I, Surveillance, and Reconnaissance Architecture. The dominant enabler for Army transformation is to attain a seamless interoperable joint C4I, surveillance, and reconnaissance architecture within the infrastructure. The Army vision starts with the Army creating processes and designing a Web-based force for individuals or organizations to obtain needed knowledge from the infrastructure. During the Army's transformation, the Web's use is to sustain and improve interoperability across all Army components, within the Joint team and with multinational partners. Army transformation efforts will produce the Objective Force systems with the

Future Combat Systems as the centerpiece. The Objective Force will have embedded autonomous, self-synchronizing automated capabilities to support the Joint Force. The Army faces a complex challenge in achieving an effective coexistence between interoperability and IA within the context of many planning documents such as the Joint Vision 2020, the GIG, and the Army Transformation Roadmap.

Scope of Army Programs Surveyed. We judgmentally selected 41 new or modified Army programs with research and development funding that interface with other systems. We sent a questionnaire to each program office to survey their awareness of interoperability and IA requirements. Appendix D contains the results of the survey. In addition, we requested each program office to provide the following documents:

- operational requirements document (ORD),[1]
- C4I Support Plans,
- test and evaluation master plans (TEMP), and
- system security authorization agreements (SSAA).

Appendix E lists the Army programs surveyed.

Overall Audit Project. This project is a continuation of work begun on Project No. D2002AE-0009, "Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems," which addressed whether the Office of the Secretary of Defense and the Defense agencies were effectively implementing DoD interoperability and IA policies. Subsequent audits are planned to address the adequacy of interoperability and information assurance requirements for systems in the Navy and the Air Force, and used by the unified combatant commands.

Objectives

The primary audit objective was to evaluate whether the Army was effectively implementing DoD interoperability and IA policies. The audit determined whether the Army was effectively identifying system interoperability and IA requirements in the requirements generation process. See Appendix A for a discussion of the audit scope and methodology, and prior coverage related to the audit objectives.

[1]DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003, states that, during system development and demonstration, the capability development document instead of the ORD will have the detailed operational performance parameters. Further, the Instruction states that the capability production document instead of the ORD will have the operational requirements resulting from system development and demonstration and will detail the performance expected of the production system. However, this report uses the term ORD because the programs reviewed during the audit used ORDs.

A. Compliance With the Global Information Grid

The Army did not implement DoD policy that required the Army to define how each Army system will interface within the GIG to achieve joint interoperability. DoD policy was not implemented because the Secretary of the Army, or his designated representative, did not:

- issue guidance to comply with the DoD GIG policy;
- populate and maintain the Army's portion of the GIG asset inventory; and
- provide Army program offices and combat developers[2] at the Army Training and Doctrine Command (TRADOC) with training that addresses policy and compliance issues related to the GIG.

Without a defined policy depicting how each Army system will interface within the GIG, the Army has not ensured that its systems have the most effective, efficient, and secure information-handling capabilities available, consistent with national military strategy, operational requirements, and best-value enterprise-level business practices.

Global Information Grid Policy

DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002, and DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003, provide policy concerning the GIG.

DoD Directive. DoD Directive 8100.1 establishes policy and assigns responsibilities for GIG configuration management and architecture and applies to the Office of the Secretary of Defense as well as the Military Departments. The Directive states that the DoD Components will plan, resource, acquire, and implement the GIG in accordance with the DoD Directives System 5000 series. The Directive requires GIG assets to be interoperable to meet the requirements of approved requirements documents and to comply with the operational, system, and technical architecture views. Before DoD issued DoD Directive 8100.1, the above requirements were included in DoD Memorandum, "DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001," March 31, 2000.

DoD Instruction. DoD Instruction 5000.2 requires the DoD Chief Information Officer to lead the development and facilitate the implementation of the GIG

[2]Army Regulation 71-9 states that the Army Training and Doctrine Command is the Army combat developer, who serves as the user representative for system acquisitions. The combat developer is responsible for development and approval of materiel requirements, as well as, doctrine and organization.

Integrated Architecture, which supports all mission area and capability architectures.[3] Further, the Instruction requires the Military Departments and the Defense Agencies to participate in the identification of the appropriate technical view consisting of standards that define and clarify the individual systems technology and integration requirements. The Instruction also requires the acquisition of all information technology systems to be consistent with the GIG policies. The combat developer for each system is to document a key performance parameter for interoperability requirements in the ORD.

Implementing Global Information Grid Policy in ORDs

The Army did not implement DoD policy that required the Army to define how each Army system will interface within the GIG to achieve interoperability. DoD policy was not implemented because the Secretary of the Army, or his designated representative, did not provide direction to Army user representatives to implement the DoD GIG policy in the requirements generation process. Because combat developers at TRADOC lacked awareness of their GIG requirements, 33 of the 41 Army programs surveyed had ORDs that did not include requirements identifying how the systems would interface within the GIG.

Combat Developers Awareness of the GIG. Combat developers at the TRADOC were not fully aware of how to implement the GIG requirements. The TRADOC stated that combat developers were adding boilerplate statements for the GIG capstone requirements document and hoping to build software with common specifications, standards, or processes. Interviews with six directorates of combat development established that each combat developer had a different understanding of how to comply with GIG requirements. In addition, TRADOC personnel stated that they did not have a database or tool for tracking ORDs to determine which systems were required to interface within the GIG.

Complying with GIG Policy. During the requirements definition and development stage, the combat developers are required to link the ORD to the appropriate CRD. The GIG Capstone Requirements Document states that the GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services;

[3]The June 2001 and April 2002 versions of DoD Regulation 5000.2-R required the DoD Chief Information Officer's acquisition-related responsibilities to focus on key principles such as the operational view of the approved GIG Integrated Architecture and the approved GIG CRD. The review was to focus on compliance with GIG-related policies and the approved GIG Integrated Architecture. The principal participants at DoD Chief Information Officer reviews include the cognizant program executive officer and program manager and Component acquisition executives and chief information officers of the Military Departments. Further, the Regulation required that the C4I support plan provide a qualitative assessment addressing the GIG integrated architecture and relevant mission area integrated architectures.

- provides retention, organization, visualization, IA, or disposition of data, information, or knowledge received from or transmitted to other equipment, software, and services; or

- processes data or information for use by other equipment, software, or services.

Further, the GIG Capstone Requirements Document requires that an ORD for new systems and for upcoming legacy systems that are associated with GIG systems, regardless of acquisition category, must comply with the GIG Capstone Requirements Document.

Applicability of the GIG Capstone Requirements Document. The GIG Capstone Requirements Document applies to the 41 systems surveyed because those systems interoperate with other systems. Consequently, we reviewed the ORDs obtained from the 41 program offices to determine whether the combat developers addressed GIG requirements during the requirements generation process. Although required, combat developers had updated only 24 of the 41 ORDs after the GIG Capstone Requirements Document was issued on August 30, 2001. Further, combat developers linked only eight of the updated ORDs to the GIG capstone requirements documents.

GIG Asset Inventory

GIG Asset Inventory Policy. DoD Directive 8100.1 requires the DoD Components to populate and maintain their portion of the GIG asset inventory; and acquire or procure, in compliance with the GIG architecture, all leased, owned, operated, or managed GIG systems, services, upgrades, or expansions to existing systems or services.

Army GIG Asset Inventory. Personnel in the Army Chief Information Office stated that the Army had not compiled an inventory of GIG assets to comply with DoD Directive 8100.1. Although no Army GIG asset inventory existed, we asked the 41 Army program offices surveyed whether they considered their programs to be part of the GIG asset inventory. The program offices responses were as follows:

- 17 Army program offices responded that their programs were part of the GIG asset inventory,

- 11 Army program offices responded that their programs were not part of the GIG asset inventory, and

- 13 Army program offices were not sure whether their programs were part of GIG asset inventory.

Appendix D contains the complete results of the program offices' survey.

Efforts to Establish a GIG Asset Inventory. The Army Chief Information Officer is defining the Army Joint Technical Architecture.[4] Part of that effort is the Army Enterprise Infostructure Transport, which is a three-phased approach that will outline how each Army system will interface within the GIG to achieve joint interoperability.

- Phase I will stand up enterprise network transport, which will document, model, and analyze the network topology and primary interfaces of Army networks;
- Phase II will integrate and optimize subnetworks and develop a migration strategy to integrate the Army networks into a single network; and
- Phase III will establish enterprise storage and core common services that will consolidate network services, application hosting, data storage, and network management.

After the Army Chief Information Office establishes the Army Enterprise Infostructure-Transport, it will compile the Army GIG asset inventory.

GIG Training

The Army Director of Information Operations Space and Networks, Office of the Chief Information Officer agreed that the majority of combat developers did not understand how their systems interfaced within the GIG. Because the GIG is a major part of interoperability, awareness of the GIG is essential for the Services to achieve total joint interoperability as outlined in Joint Vision 2020. To correct this knowledge deficiency, the Director believed that training should be provided to combat developers and program managers on how the GIG works and how their respective systems interface within the GIG.

Although GIG training for the combat developers is needed, Army-wide training has not been provided. Personnel from the Army Chief Information Office stated that training the combat developers and program managers before the Army defines how each Army system will interface within the GIG and coordinates policies and procedures with the GIG Capstone Requirements Document would be premature. Further, the personnel stated that until the Army establishes its Joint Technical Architecture, the combat developers may not be able to fully comply with GIG requirements and provide all needed training.

[4]The Joint Technical Architecture is a common set of mandatory information technology standards, which are primarily interface standards and guidelines to be used by all emerging systems and systems upgrades, including advanced concept technology demonstrations.

Effect on Implementing the Global Information Grid Policy

Without a defined policy depicting how each Army system will interface within the GIG, the Army cannot ensure that its systems have the most effective, efficient, and assured information-handling capabilities available, consistent with national military strategy, operational requirements, and best-value enterprise-level business practices.

Management Comments on the Finding

Although not required to comment, the Director, Operational Test and Evaluation agreed with the finding. For the complete text of the Director's comments, see the Management Comments section of the report.

Recommendations and Management Comments

A. We recommend that the Secretary of the Army:

1. Issue and implement guidance to comply with DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002, which requires the Army to define how each Army system will interface within the Global Information Grid to achieve joint interoperability.

Principal Director for Enterprise Integration, Office of the Army Chief Information Officer Comments. The Principal Director, responding for the Secretary of the Army, concurred, stating that the Army is revising Army Regulation 25-1, "Army Information Management," May 31, 2002, and Army Regulation 70-1, "Army Acquisition Policy," December 15, 1997, to include the requirements of DoD Directive 8100.1. Further, he stated that any requirements not adequately addressed will be incorporated into the next revision of those regulations. The Principal Director also stated that the Army published its Army Knowledge Implementation Plan in September 2003 and the next revision of the plan will address how Army systems will interface with the GIG. For the complete text of the Principal Director's comments, see the Management Comments section of the report.

Director, Operational Test and Evaluation Comments. Although not required to comment, the Director agreed with the recommendation. For the complete text of the Director's comments, see the Management Comments section of the report.

2. Expedite efforts to populate and maintain the Army's portion of the Global Information Grid asset inventory in accordance with DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002.

Principal Director for Enterprise Integration Comments. The Principal Director concurred, stating that the Army expects to complete documenting its information technology assets by the end of the first quarter of FY 2004. Further, he stated that the Army will develop an enterprise management strategy to oversee those information technology assets by the end of the second quarter of FY 2004 and expects to implement the strategy in the first quarter of FY 2005.

Director, Operational Test and Evaluation Comments. Although not required to comment, the Director agreed with the recommendation.

3. Provide Army combat developers at the Army Training and Doctrine Command with training on how to implement the requirements of the Global Information Grid.

Principal Director for Enterprise Integration Comments. The Principal Director concurred, stating that, using the strategy outlined in the Army Knowledge Management Goals, the Army will provide guidance to the Army Training and Doctrine Command on how to develop training to implement GIG requirements by the end of the fourth quarter of FY 2004.

Director, Operational Test and Evaluation Comments. Although not required to comment, the Director agreed with the recommendation.

B. Implementing Interoperability Policies

The Army requirements community did not adequately address interoperability in the requirements generation process for use in the acquisition process. Interoperability was not adequately addressed because the Army Deputy Chief of Staff for Operations and Plans, in coordination with Army Chief Information Office, did not update Army regulations pertaining to system acquisitions to implement DoD and Joint Staff interoperability requirements for:

- combat developers to identify interoperability requirements in requirements documents and to update the requirements throughout the life of the systems, as necessary;
- program managers to use C4I support plans to document interoperability and supportability requirements; and
- program managers to obtain Director, Command, Control, Communications, and Computer Systems Directorate (J-6) (the Joint Staff J-6) validation of system warfighter interoperability requirements.

Without updating Army regulations to effectively implement DoD interoperability policy, the Army risks developing systems that operate independently of other Army and DoD systems and not realizing the full benefits of interoperable DoD systems that conform to the GIG and satisfy the needs of the warfighter as outlined in Joint Vision 2020.

Interoperability Requirements

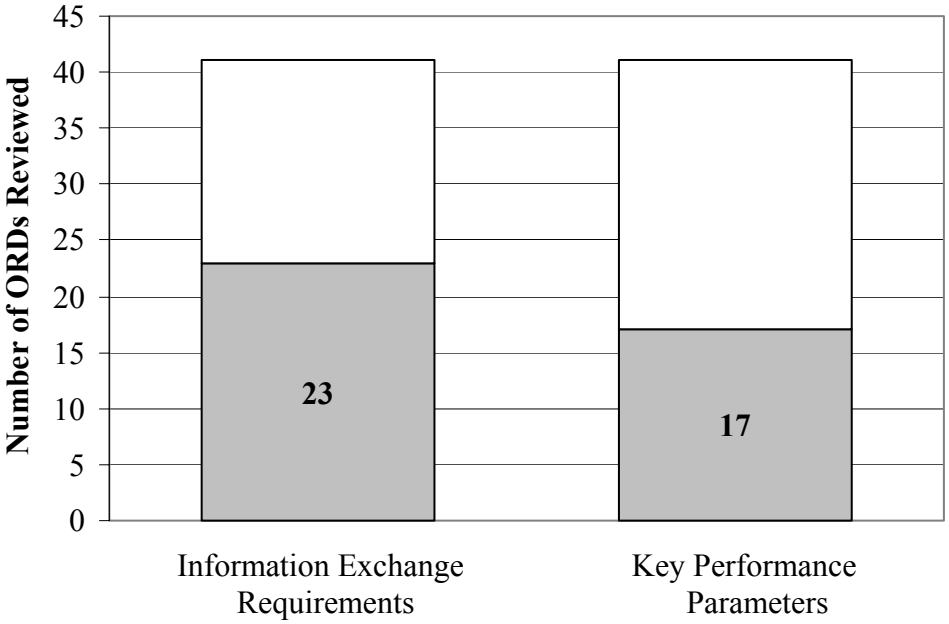
The Army did not consistently include interoperability requirements in its requirements documents because the Army Deputy Chief of Staff for Operations and Plans, in coordination with the Army Chief Information Officer, had not updated its implementing regulations for interoperability. As a result, combat developers for only 15 of the 41 Army program offices surveyed had included testable interoperability key performance parameters and information exchange requirements in ORDs.

DoD Interoperability Requirements Policy. DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" January 11, 2002, as implemented in DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 2, 2002, require the DoD Components to identify interoperability and supportability requirements for information technology and National Security (NS) systems during the acquisition process and update as necessary throughout the system's life. Specifically, DoD policy requires the DoD Components to define and develop information exchange requirements and interoperability key performance

parameters. The information exchange requirements characterize the information exchanges to be performed by the proposed system. The interoperability key performance parameter defines the level of interoperability for the proposed system and will be derived from the information exchange requirements. The interoperability key performance parameter is to be measurable and testable.[5]

Review of Operational Requirement Documents. Based on our review of the ORDs for the 41 Army programs surveyed, we determined whether the combat developers included information exchange requirements and associated interoperability key performance parameters that could be measured, tested, and evaluated. The following table shows the number of Army programs surveyed that did not have information exchange requirements and associated interoperability key performance parameters.

Interoperability Requirements Not Established in ORDs.



In addition, of the 24 ORDs that included interoperability key performance parameters, 16 ORDs had key performance parameters that could be measured, tested, and evaluated.

According to Joint Staff policy memorandum, "Policy for Updating Operational Requirements Documents to Incorporate the Interoperability Key Performance Parameter and Cost," November 16, 1999, all ORDs supporting a system development and demonstration or production and deployment milestone

[5]Measurable and testable key performance parameters are parameters that testers can use to measure, test, and evaluate the obtainment of system objectives and thresholds.

decision[6] after March 1, 2001, will be updated to include information exchange requirements and interoperability key performance parameters.

Updated Army Interoperability Requirements. The Army did not consistently include interoperability requirements in its requirements documents because the applicable Army ORD preparation guidance was not up-to-date. Army Regulation 71-9, "Materiel Requirements," April 30, 1997, provides Army policy and procedures for materiel warfighting requirements and assigns the Army Deputy Chief of Staff for Operations and Plans with the responsibility for updating and maintaining the Regulation.

On February 21, 2000, the Army Deputy Chief of Staff for Operations and Plans issued a memorandum, "Policy for Updating Operational Requirements Documents (ORDs) to Incorporate Interoperability Key Performance Parameters (KPPs) and Costs," which states that all requirements documents currently in the approval process, regardless of acquisition category, must include interoperability key performance parameters as required in the previous version of Chairman of the Joint Chiefs of Staff Instruction 3170.01B, "Requirements Generation System," April 15, 2001.[7] The requirements documents that are receiving funding must be updated by October 1, 2000.

On April 12, 2001, the Army Deputy Chief of Staff for Operations and Plans issued a memorandum, "Approval of Army Warfighting Requirements–Interim Implementation Guidance," that serves as interim guidance pending an update to Army Regulation 71-9, which was last updated April 30, 1997. The interim guidance applies to all requirements documents regardless of acquisition category. However, the Regulation and the interim guidance do not require the Army combat developers to identify interoperability and supportability requirements for information technology and NS systems during the requirements generation process and to update the requirements as necessary throughout the system's life, in accordance with DoD Policy.

Although the Army Deputy Chief of Staff for Operations and Plans issued a few policy memorandums, the Army Deputy Chief of Staff for Operations and Plans has not updated Army Regulation 71-9 since 1997. The Army Deputy Chief of Staff for Operations and Plans needs to update the regulation to incorporate the interoperability requirements. If combat developers do not identify interoperability key performance parameters in the ORDs, program managers cannot incorporate those interoperability requirements into the C4I support plans and the TEMPs.

[6] As of the date of the policy memorandum, the system development and demonstration milestone and production and deployment milestone were referred to as Milestone II and Milestone III, respectively.

[7] Subsequent to the issuance of the draft audit report, the Joint Staff issued Chairman of the Joint Chiefs of Staff Instruction 3170.01C, "Joint Capabilities Integration and Development System," June 24, 2003, which canceled Chairman of the Joint Chiefs of Staff Instruction 3170.01B.

C4I Support Plans

DoD Instruction 4630.8 requires program managers to prepare a C4I support plan to document interoperability and supportability requirements. The C4I support plan is a mechanism to identify and resolve implementations issues related to C4I surveillance and reconnaissance infrastructure and interface requirements. DoD Instruction 4630.8 also requires program managers to:

- prepare the initial C4I support plan before the system development and demonstration milestone decision and
- maintain the C4I support plans throughout the acquisition life cycle.

At each milestone review, C4I support plans are to contain progressively more detailed and specific time-phased descriptions of the types of information needed: operational, systems, and technical architecture views; security, connectivity, and interoperability issues; and infrastructure and support shortfalls.

Review of C4I Support Plans. Based on our review of the 41 Army programs surveyed, we determined that Army program managers were not, for the most part, preparing C4I support plans. Specifically, we requested C4I support plans from the 41 Army program offices.[8] Thirty-seven of the 41 Army programs were past the system development and demonstration milestone decision. As a result, the program managers for those 37 programs should have prepared a C4I support plan. However, program managers for only 13 of the 37 programs had a C4I support plan.

C4I Support Plan Requirement. Although DoD policy states that program managers for all acquisition systems past the system development and demonstration milestone decision should have a C4I support plan, the 24 other Army program offices stated that they did not prepare a C4I support plan because:

- the program had entered full-rate production before the C4I support plan became a requirement (11 program offices);
- the program was part of another program (1 program office);
- the cost to prepare a C4I support plan was not justifiable (1 program office);
- the program did not interface with other programs (3 program offices); and
- the program office planned to prepare or was beginning to prepare a C4I support plan (8 program offices).

[8]We requested C4I support plans by a data request and followed up with phone calls to the program offices to verify that C4I support plans did not exist. In addition, we contacted the Office of the Army Chief Information Officer to obtain C4I support plans.

In addition, the Army Deputy Chief of Staff for Operations and Plans, in coordination with Army Chief Information Office, had not updated Army acquisition regulations to conform with DoD policy. Specifically, Army Regulation 70-1, "Army Acquisition Policy," December 15, 1997, which implements the Army's acquisition policy for all Army acquisition programs, and Army Regulation 71-9 do not require Army program managers for all acquisition programs to prepare a C4I support plan to document interoperability and supportability requirements, as required by DoD Instruction 4630.8. Accordingly, Army program managers were not benefiting from preparing C4I support plans to describe system dependencies and interfaces in sufficient detail to enable them and operational testers to test interoperability key performance parameters derived from information exchange requirements.

Interoperability Certification Process

Interoperability is essential for seamless and effective operations of joint, combined, and coalition forces. To implement, DoD established an interoperability certification process to ensure that joint information technology and NS systems conform to DoD policy, doctrine and interoperability standards. However, the Army Deputy Chief of Staff for Operations and Plans, in coordination with Army Chief Information Officer, did not implement procedures for the interoperability certification process. As a result, Army program managers did not always obtain the required interoperability requirements and supportability certifications and validations from the Joint Staff J-6. The Joint Staff J-6 certification and validation process consists of the following three forms of capability confirmation:

- interoperability requirements certification,
- supportability certification, and
- interoperability system validation.

Joint Staff J-6 Interoperability Requirements Certification. Chairman of the Joint Chiefs of Staff Instruction 6212.01B, "Interoperability and Supportability of National Security Systems, and Information Technology Systems," May 8, 2000,[9] requires the Joint Staff J-6 to certify interoperability requirements in the ORDs before milestone decisions of system acquisition programs. The Joint Staff J-6 certifies mission need statements, CRDs, and ORDs, regardless of acquisition category level, for conformance with joint information technology and NS system policy and doctrine and interoperability standards. As part of the review process, the Joint Staff J-6 requests assessments from the Military Departments, the Defense Information Systems Agency, and other DoD agencies through the Joint Staff J-6 assessment tool.

[9] According to the Joint Staff, the Chairman of the Joint Chiefs of Staff Instruction 6212.01B, "Interoperability and Supportability of National Security Systems, and Information Technology," May 8, 2000, is being updated for issuance in November 2003.

Results of Interoperability Requirements Certification. We reviewed the 41 Army programs surveyed to determine whether combat developers had the Joint Staff J-6 certify the interoperability requirements in their ORDs. Of the 41 programs, 11 combat developers had obtained the required interoperability requirements certification and 7 combat developers had entered their ORDs into the interoperability requirements certification process within the last year. Of the remaining 23 programs reviewed:

- 13 combat developers had their ORDs in the interoperability requirements certification process for more than 1 year without any advancement, and

- 10 combat developers did not submit their ORDs to the Joint Staff J-6 for review in the interoperability requirements certification process.

According to the Office of the Army Deputy Chief of Staff for Operations and Plans, 22 of the 23 programs were not being formally updated in preparation for a milestone decision review, so the ORDs did not need to be submitted to the Joint Staff J-6 for the interoperability requirements certification process.

However, 9 of the 23 programs had milestone decisions since the issuance of Joint Staff policy or have upcoming milestone decisions within the next year; therefore, we determined that the ORDs should have been updated or should be updated to include information exchange requirements and an interoperability key performance parameters. Further, the ORDs should have been subjected or should be subjected to interoperability requirements certification. In addition, 19 of the 23 programs were budgeted for funding in FY 2003 and, according to the February 21, 2000, Army Deputy Chief of Staff for Operations and Plans policy memorandum, requirements documents should be updated and interoperability certification obtained.

Joint Staff J-6 Supportability Certification. Chairman of the Joint Chiefs of Staff Instruction 6212.01B requires the Joint Staff J-6 to certify to the Assistant Secretary of Defense (Networks and Information Integration)[10] that C4I support plans, regardless of acquisition category, adequately address information technology and NS system infrastructure requirements, the availability of bandwidth and spectrum support, funding, and personnel, and also identify dependencies and interface requirements among systems. As part of the review process, the Joint Staff J-6 requests supportability assessments from the Defense Information Systems Agency and other DoD agencies through the Joint Staff J-6 assessment tool. Further, DoD Instruction 4630.8 requires that the Joint Staff J-6 conduct a supportability certification of C4I support plans before milestone decisions for submission to the Assistant Secretary of Defense (Networks and Information Integration) as part of the C4I support plan review process.

[10]Formerly named the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

Results of Joint Staff J-6 Supportability Certification. Of the 17 C4I support plans obtained for the 41 Army programs surveyed, as discussed earlier:

- 3 program managers had received the required supportability certification of their C4I support plans from the Joint Staff J-6 ,
- 2 program managers had their C4I support plans in the supportability certification process for more than 1 year without any advancement, and
- 12 program managers did not submit their C4I support plans to the Joint Staff J-6 for review in the supportability certification process.

Even though Chairman of the Joint Chiefs of Staff Instruction 6212.01B requires the Joint Staff J-6 to certify C4I support plans, regardless of acquisition category, personnel in the Army Chief Information Office were of the opinion that only Acquisition Category I programs are required to have their C4I support plans certified by the Joint Staff J-6.

Joint Staff J-6 Interoperability System Validation. Chairman of the Joint Chiefs of Staff Instruction 6212.01B states that the Joint Staff J-6 validation is intended to provide total life-cycle oversight of warfighter interoperability requirements, which occurs after the Joint Staff J-6 interoperability requirements and supportability certifications. As part of the system validation process, the program managers are required to submit their systems to the Joint Interoperability Test Command (JITC) for interoperability testing and certification. Further, the Instruction states that the Joint Staff J-6 is to validate the JITC interoperability system test results 15 days after the JITC certification. According to the Instruction, Military Departments and Defense agencies are required to have those systems undergo interoperability certification testing before the full-rate production decision approval for all new or modified information technology and NS systems.

Results of Interoperability System Validation. Of the 41 programs surveyed, 11 programs had a production and fielding milestone decision since May 2000, when the Chairman of the Joint Chiefs of Staff Instruction 6212.01B was issued. However, none of the program managers had obtained the Joint Staff J-6 interoperability validation for their systems as required by the Joint Staff policy discussed above.

Furthermore, eight program managers requested JITC to perform interoperability testing before obtaining Joint Staff J-6 certification of the interoperability requirements contained in the ORD, as required by Joint Staff policy. As a result, JITC tested four of the eight programs without Joint Staff J-6 interoperability requirements certifications and certified three of those programs. Thus, four programs were prematurely tested before the Joint Staff J-6 certified the interoperability requirements, coordinated the requirements with the other Military Departments and Defense agencies, or ensured that the interoperability requirements complied with joint policy, doctrine, and interoperability standards.

Need to Complete the Interoperability Certification Process. Army program managers need to obtain the required interoperability requirements certification of ORDs, the supportability certification of C4I support plans, and the interoperability system validation from the Joint Staff J-6 to ensure that the warfighter has effective, integrated systems and networks that meet mission needs.

Effects of Army Implementation of DoD Interoperability Policy

Without updating Army regulations to effectively implement DoD interoperability policy, the Army risks developing systems that operate independently of other Army and DoD systems and not realizing the full benefits of interoperable DoD systems that conform to the GIG and satisfy the needs of the warfighter as outlined in Joint Vision 2020.

Management Comments on the Finding

Although not required to comment, the Director, Operational Test and Evaluation agreed with the finding. For the complete text of the Director's comments, see the Management Comments section of the report.

Recommendations, Management Comments, and Audit Response

B. We recommend that the Army Deputy Chief of Staff for Operations and Plans, in coordination with the Army Chief Information Officer, update Army Regulation 70-1, "Army Acquisition Policy," December 15, 1997, and Regulation 71-9, "Materiel Requirements," April 30, 1997, to require that:

1. Combat developers identify interoperability and supportability requirements in requirements documents and update the requirements throughout the life of the systems, as necessary, in accordance with DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" January 11, 2002.

2. Program managers use command, control, communications, computers, and intelligence support plans to document interoperability and supportability requirements in accordance with DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 2, 2002.

3. Program managers obtain the Joint Staff J-6 certifications for interoperability in accordance with Chairman of the Joint Chiefs of Staff Instruction 6212.01B, "Interoperability and Supportability of National Security Systems, and Information Technology Systems," May 8, 2000.

Army Deputy Chief of Staff for Operations and Plans Comments. The Deputy Chief of Staff did not provide comments on the draft report. We request that the Deputy Chief of Staff provide comments in response to the final report.

Principal Director for Enterprise Integrations Comments. The Principal Director, responding for the Army Chief Information Officer, concurred, stating that the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) and the Army Deputy Chief of Staff for Operations and Plans have begun to update Army Regulations 70-1 and 71-9 and expect to publish the updates by early FY 2004 and mid-FY 2004, respectively. He stated that the recommendations will be incorporated into the updates; however, he noted that the program managers should not be obtaining interoperability certifications, as addressed in Recommendation B.3., unless by exception.

The Principal Director also stated that interoperability certifications should be conducted when the requirements or capabilities documentation is provided to the Joint Staff for review and should include certification by the Joint Staff J-6, in accordance with Chairman of the Joint Chiefs of Staff Instruction 6212.01B, which will be replaced by Chairman of the Joint Chiefs of Staff Instruction 6212.01C. In addition, he stated that the interoperability certification, as described, is part of the new Chairman of the Joint Chiefs of Staff Instruction 3170.01C, "Joint Capabilities Integration and Development System," June 24, 2003, and was a requirement in Chairman of the Joint Chiefs of Staff Instruction 3170.01B. For the complete text of the Principal Director's comments, see the Management Comments section of the report.

Audit Response. Except for his qualification on obtaining interoperability certifications, the Principal Director's comments are responsive. Chairman of the Joint Chiefs of Staff Instruction 3170.01C and Chairman of the Joint Chiefs of Staff Instruction 6212.01B require program managers to obtain interoperability certifications. Chairman of the Joint Chiefs of Staff Instruction 3170.01C states that, for capability development documents and capability production documents (previously referred to as ORDs), interoperability and supportability certifications for National Security (NS) and information technology systems will be performed in accordance with Chairman of the Joint Chiefs of Staff Instruction 6212.01B, DoD Directive 4630.5, and DoD Instruction 4630.8.

Chairman of the Joint Chiefs of Staff Instruction 6212.01B. Chairman of the Joint Chiefs of Staff Instruction 6212.01B requires the Joint Staff J-6 to certify all NS and information technology systems as interoperable with other NS and information technology systems with which they exchange information. This interoperability certification process addresses system interoperability requirements, supportability, and total life-cycle oversight of warfighter interoperability requirements.

DoD Directive 4630.5. DoD Directive 4630.5 requires that certification of NS and information technology systems will be cost-effective and completed before new NS and information technology systems or new capabilities or upgrades to existing NS and information technology systems are fielded.

DoD Instruction 4630.8. DoD Instruction 4630.8 requires the DoD Components to certify which of the interoperability criteria have been met before production and fielding approval for all new or modified NS and information technology systems. Further, the Instruction requires the Chairman of the Joint Chiefs of Staff, with the assistance of the Defense Information Systems Agency, to certify that interoperability and supportability requirements for NS and information technology systems are established, assessed, and verified for NS and information technology systems acquisitions before production and fielding.

Accordingly, we request that the Principal Director clarify his response on program managers obtaining interoperability certifications on an exception basis.

Director, Operational Test and Evaluation Comments. Although not required to comment, the Director agreed with the recommendation. For the complete text of the Director's comments, see the Management Comments section of the report.

C. Information Assurance Testing of Army Systems

The Army testers did not consistently conduct IA testing for Army acquisition programs because:

- TRADOC, as the combat developer, did not coordinate with the Army Test and Evaluation Command to fully identify IA requirements in ORDs for testing Army programs with interoperability and supportability requirements;
- combat developers at TRADOC were not aware of their roles and responsibilities in implementing the DoD Information Technology Security Certification and Accreditation Process (DITSCAP);
- the Army Chief Information Officer did not verify that program managers for Army acquisition programs with information technology requirements prepared and maintained an SSAA in accordance with the DITSCAP; and
- the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) did not require SSAA signatories[11] to coordinate with the Army Test and Evaluation Command throughout the acquisition cycle to minimize duplicative IA testing efforts for Army systems subject to the DITSCAP.

As a result, milestone decision authorities could not be assured that systems developed satisfied the IA requirements of availability, integrity, authenticity, confidentiality, and nonrepudiation of information to meet warfighter requirements as envisioned in the Quadrennial Defense Review and Joint Vision 2020.

Defining Information Assurance Requirements for Testing

TRADOC did not fully identify IA requirements in ORDs for testing Army acquisition programs with interoperability and supportability requirements because TRADOC did not coordinate with the Army Test and Evaluation Command when developing and updating ORDs. As a result, combat developers for only 3 of the 41 Army program offices surveyed included testable IA requirements[12] in the applicable ORDs.

[11]The SSAA signatories include the information technology system program manager, the designated approving authority, the certification authority, and the user representative.

[12]Testable IA requirements are written in output-oriented and measurable terms in threshold and objective format with criteria and rationale for each.

Information Assurance Requirements Policy. DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003, requires acquisition managers to address IA for all weapons, C4I surveillance and reconnaissance, and information technology programs that depend on external information sources or that provide information to other DoD systems. In addition, DoD Instruction 5000.2 requires operational tester and evaluators to assess those programs. Further, Chairman of the Joint Chiefs of Staff Instruction 3170.01B, "Requirements Generation System," April 15, 2001,[13] requires all DoD systems that are used to enter, process, store, display, or transmit DoD information regardless of classification or sensitivity to address IA. The Instruction also requires the initial ORD to establish requirements describing the capabilities and characteristics of the proposed system. Further, the Instruction states that the requirements must be written in output-oriented and measurable terms in threshold and objective format, with criteria and rationale for each.

In addition, DoD Directive 4630.5; DoD Directive 8500.1, "Information Assurance," October 24, 2002; DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003; DoD Guidebook, "Interim Defense Acquisition Guidebook," October 30, 2002; Army Regulation 70-1; and Army Regulation 73-1, "Test and Evaluation Policy," January 7, 2002, establish additional requirements and guidance for IA requirements generation and for testing. Appendix F discusses the additional requirements and guidance.

Testable Information Assurance Requirements. Based on our review of the 41 Army programs surveyed, we determined whether the applicable ORDs and the corresponding TEMPs had IA requirements that could be measured, tested, and evaluated. Although 22 of the 41 ORDs contained IA requirements, only 3 of them were written in output-oriented and measurable terms.

Identifying Information Assurance Requirements for Testing. TRADOC did not always identify testable IA requirements in ORDs for Army programs with interoperability and supportability requirements. Conversely, in a substantial number of instances, the Army Test and Evaluation Command did identify IA requirements for testing in system evaluation plans (SEPs),[14] even when the ORD did not identify those requirements

Army Training and Doctrine Command. Although required by Chairman of the Joint Chiefs of Staff Instruction 3170.01B and the TRADOC requirements generation guidance, TRADOC personnel stated that they did not require subordinate elements to develop testable IA requirements in ORDs for Army programs with interoperability and supportability requirements.

[13]Subsequent to the issuance of the draft audit report, the Joint Staff issued Chairman of the Joint Chiefs of Staff Instruction 3170.01C, "Joint Capabilities Integration and Development System," June 24, 2003, canceled Chairman of the Joint Chiefs of Staff Instruction 3170.01B.

[14]The SEP documents the integrated test and evaluation strategy, which is the evaluation strategy and the test and simulation execution strategy that the testers and evaluators use throughout the system acquisition life cycle.

For direction in preparing an ORD, TRADOC issued a "Guide for Development of Army Operational Requirements Documents," October 2002, that provides a mandatory format for all Army-developed ORDs. The Guide requires the Directorates of Combat Development, as the user representatives, to address the defensive measures needed to ensure that IA requirements include availability, integrity, authentication, confidentiality, and nonrepudiation of the information to be exchanged and used. However, the Guide does not require user representatives to coordinate with Army testers to verify that IA requirements included in the ORDs are testable.

Army Test and Evaluation Command. To determine whether IA requirements in ORDs could be measured, tested, and evaluated, we contacted personnel from the Army Test and Evaluation Command, including representatives from the Army Evaluation Center, who are responsible for evaluating developmental and operational test results, and the Army Operational Test Command Headquarters, who are responsible for conducting operational testing.

Army Evaluation Center. Army Evaluation Center personnel stated that, when ORDs for systems with interoperability and supportability requirements did not identify testable IA requirements, they added testable IA requirements into the "Additional Issues" section of the respective program's SEP and the subsequent system evaluation report (SER)[15] for testing and evaluating the system's IA capabilities. We reviewed the SEP or SER for 9 of the 41 programs surveyed. For six of the nine programs, the Army Evaluation Center added IA requirements in the "Additional Issues" section of the SEPs or SERs.[16] For the remaining three programs, the Army Evaluation Center addressed IA requirements in other sections of the SEPs or SERs.

Army Operational Test Command Headquarters. To determine the effect that not having testable IA requirements in ORDs had on operational test results, we met with three of the Army Operational Test Command's subordinate directorates: the Command, Control, Communications, and Computers Test Directorate, the Information and Electronic Warfare Test Directorate, and the Air Defense Artillery Test Directorate.

Command, Control, Communications, and Computers Test Directorate. The IA procedures at the Command, Control, Communications, and Computers Test Directorate (the Directorate) required the operational testers to plan and conduct operational testing of IA requirements in the ORD for C4I acquisition programs only. For non-C4I acquisition programs, the Directorate used a draft test checklist to assess IA during operational testing. However, Directorate personnel advised that other subordinate directorates of the Army Operational Test Command did not universally use the draft IA test checklist.

[15]The SER documents independent evaluation findings and recommendations on system operational effectiveness, suitability, and survivability.

[16]The SEPs and SERs were from separate programs.

Information and Electronic Warfare Test Directorate. Personnel at the Information and Electronic Warfare Test Directorate (the Directorate) stated that their ability to test IA requirements for Army systems is impaired when the ORDs for Army systems omit testable IA requirements. In those cases, the Directorate cannot conduct tests to determine whether the IA for those systems are operationally effective, suitable, and survivable for the intended use by the warfighter.

Air Defense Artillery Test Directorate. Personnel at the Air Defense Artillery Test Directorate also stated that, when the ORDs for Army systems omitted testable IA requirements, they were unable to conduct tests to determine whether the IA for those systems were operationally effective, suitable, and survivable for the intended use by the warfighter.

Combat Developer Awareness of DITSCAP Requirements

Combat developers at TRADOC were not aware of their roles and responsibilities in implementing the DITSCAP because the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) had not updated Army Regulation 70-1 to identify the roles and responsibilities of combat developers concerning DITSCAP requirements.

DITSCAP Requirements. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, establishes the DITSCAP for security certification and accreditation of unclassified and classified information technology. The DITSCAP sets forth the activities and management structure to certify and accredit information technology systems that will maintain the security posture of the Defense Information Infrastructure. Further, the Instruction states that the interests of system users are vested in the user representatives, who:

- are concerned with system availability, access, integrity, functionality, and performance;
- are the liaison for the users during the initial development of a system;
- define the system mission and functionality; and
- ensure that the user's interests are maintained throughout system development, modification, integration, acquisition, and deployment.

Army Combat Developer Involvement in the DITSCAP. Army acquisition policy did not include the DITSCAP requirements of DoD Instruction 5200.40 concerning the roles and responsibilities of user representatives. To determine the user representatives' involvement and awareness of their roles and responsibilities in the implementation of the DITSCAP, we interviewed cognizant personnel at

six Directorates of Combat Development within TRADOC. The Directorates of Combat Development were located at:

- Fort Bliss, Texas;
- Fort Benning, Georgia;
- Fort Gordon, Georgia;
- Fort Knox, Kentucky;
- Fort Leonard Wood, Missouri; and
- Fort Sam Houston, Texas.

Personnel at four of six Directorates of Combat Development stated that they were not involved in the implementation of the DITSCAP. Instead, they were of the opinion that Army program managers were responsible for implementing the DITSCAP for their respective programs. Accordingly, the Directorates of Combat Development were not exercising their required roles and responsibilities for resolving schedule, budget, security, functionality, and performance issues associated with the DITSCAP.

Preparing and Maintaining System Security Authorization Agreements

SSAA Policy. DoD Instruction 5200.40 and Army Regulation 25-1, "Army Information Management," May 31, 2002, provide policies and procedures concerning the DITSCAP, including SSAAs

DoD Instruction 5200.40. DoD Instruction 5200.40 states that the DITSCAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information. Further, the Instruction states that a critical element of the DITSCAP is the agreement among the information technology system program manager,[17] the designated approving authority, the certification authority, and the user representative to resolve critical schedule, budget, security, functionality, and performance issues. This agreement is documented in the SSAA that is used to guide and document the results of the certification and accreditation process. The SSAA establishes a binding agreement on the level of security required before system development or changes begin. The SSAA is used throughout the entire DITSCAP to guide actions, document decisions, specify information technology security requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational systems security.

[17]The term program manager refers to the acquisition organization's program manager during the system acquisition, the system manager during the operation of the system, or the maintenance organization's program manager when a system is undergoing a major change.

Army Regulation 25-1. Army Regulation 25-1 requires the Army Chief Information Officer to validate all warfighting requirements through the review of appropriate requirements documents. Validation criteria will include compliance with information security requirements. The Regulation also requires that all information systems and networks be subjected to an established certification and accreditation process, which verifies that the required levels of IA are achieved and sustained throughout their life cycle. Further, the Regulation states that information systems and networks will be certified and accredited in accordance with DoD Instruction 5200.40.

SSAA Implementation. To determine whether Army acquisition program offices with information technology requirements had an SSAA, we requested SSAAs from the program managers for the 41 Army program offices surveyed. We contacted the Army Test and Evaluation Command, which conducts the Army's operational testing and evaluation, to determine whether it was provided SSAAs for use in conducting operational testing.

SSAA Survey. In the survey questionnaire on the implementation of interoperability and IA requirements, we asked the program managers the following question concerning SSAAs: Of the following documentation normally provided to the milestone decision authority at the system development and demonstration decision point and the production and deployment decision point, which adequately describes IA requirements and strategies? In response, 19 of the 41 program managers believed that the SSAA best described the IA requirements and strategies for the system development and demonstration milestone decision and 28 of the 41 program managers believed that it best described the IA requirements and strategies for the production and deployment milestone decision (Appendix D contains the results of the survey). If the program managers do not prepare the SSAAs before milestone decision points, the milestone decision authority cannot be assured that the program manager, the designated approving authority, the certification authority, and the user have all agreed on the method for implementing information technology security requirements and maintaining operational systems security.

SSAA Request. Based on our request, 35 of the 41 Army program offices surveyed provided an SSAA. We did not determine whether the contents of the SSAAs were adequate. However, the SSAA signatories should have prepared an SSAA for all 41 programs because it is the formal agreement among the designated approving authority, the certification authority, the information technology system user representative, and the program manager to guide actions, document decisions, specify information technology security requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational systems security.

Army Test and Evaluation Command. The Army Operational Test Command and the Army Evaluation Center within the Army Test and Evaluation Command did not always receive SSAAs because the:

- Army Chief Information Officer did not ensure that program managers for Army acquisition programs with information technology

requirements prepared and maintained an SSAA in accordance with Army Regulation 25-1, and

- Assistant Secretary of the Army (Acquisition, Logistics, and Technology) had not updated Army Regulation 70-1 to require the SSAA signatories to coordinate with the Army Test and Evaluation Command throughout the acquisition cycle for Army systems subject to the DITSCAP.

Army Operational Test Command. Personnel at the Army Operational Test Command stated that Army program offices did not always provide them with SSAAs even though they made repeated requests for the SSAAs. Without an SSAA, the operational testers cannot adequately conduct IA testing to determine whether planned and implemented security measures satisfy the system's ORD and information technology security requirements. Further, the operational testers cannot determine the level of risk associated with operating the system and the extent of security testing required.

Army Evaluation Center. Personnel at the Army Evaluation Center stated that SSAAs were essential for their IA risk assessments. However, the personnel stated that they did not always receive complete SSAAs from Army program managers. The personnel attributed that condition to DITSCAP being completely separate from the acquisition process. As a result, evaluators at the Army Evaluation Center have to incorporate additional IA test requirements into their SEPs to determine whether the systems with IA requirements are operationally effective and suitable based on the systems availability, access, integrity, functionality, and performance.

Coordination of DITSCAP Testing and Program Evaluation

DITSCAP Coordination Requirements. DoD Instruction 5000.2; DoD Guidebook, "Interim Defense Acquisition Guidebook," October 30, 2002;[18] and Director, Operational Test and Evaluation memorandum, "Policy for Operational Test and Evaluation of Information Assurance," November 17, 1999, discuss the coordination of DITSCAP testing.

DoD Instruction. DoD Instruction 5000.2 requires the program manager, together with the user and test and evaluation communities, to coordinate developmental test and evaluation, operational test and evaluation, live-fire test and evaluation, family-of-systems interoperability testing, IA testing, and modeling and simulation activities into an efficient process, integrated with requirements definition and systems design and development.

DoD Guidebook. The Guidebook states that IA testing should be conducted on information systems to ensure that planned and implemented security measures satisfy ORD and SSAA requirements when the system is installed and operated in its intended environment. Further, the Guidebook states

[18]Formerly DoD Regulation 5000.2-R. The former DoD Regulation 5000.2-R will serve as the guidebook while the Defense Acquisition Policy Working Group creates a streamlined guidebook.

that the program manager, the operational test and evaluation authority, and the designated approving authority should coordinate and determine the level of risk associated with operating a system and the extent of security testing[19] required.[20]

Director, Operational Test and Evaluation Policy. Director, Operational Test and Evaluation memorandum, "Policy for Operational Test and Evaluation of Information Assurance," November 17, 1999, requires the operational test agencies for programs subject to the DITSCAP to coordinate with the SSAA signatories throughout the acquisition cycle to minimize duplicative efforts by the operational test agencies. Further, the memorandum requires the operational test agencies and the SSAA signatories to maximize opportunities to meet operational requirements through concurrent testing, particularly in DITSCAP vulnerability assessments, security tests and evaluations, and penetration testing.

Coordination and Use of DITSCAP Test Results. To determine how effectively the SSAA signatories, specifically program managers, were coordinating with the Army Evaluation Center throughout the acquisition cycle to minimize duplicative IA testing efforts, we contacted personnel from the Army Evaluation Center and reviewed SERs. The SER documents independent evaluation findings and recommendations on system operational effectiveness, suitability, and survivability that enable the milestone decision authority to make an informed decision concerning the readiness of the system for production.

Army Evaluation Center. Personnel at the Army Evaluation Center stated that the DITSCAP is a key source of data for their IA evaluations.

Input Into DITSCAP Testing. Personnel at the Army Evaluation Center stated that the Army Evaluation Center has limited input into DITSCAP testing and that its input to the DITSCAP depends on the individual program manager. Although the DITSCAP does not define a role for the Army Test and Evaluation Command, the personnel stated that the Army Evaluation Center identifies the IA requirements for the test and evaluation process and informs the program manager when the Army Test and Evaluation Command will conduct an IA evaluation on the system. The Army Evaluation Center relies on DITSCAP testing to assess whether the system satisfied IA requirements; however, the personnel stated that program managers did not always provide the results of the DITSCAP test results in time for inclusion in their SER. As a result, not all Army SERs contain an evaluation of whether the system satisfies IA requirements.

Specific Army Guidance. Army Pamphlet 73-1, "Test and Evaluation in Support of System Acquisition," February 28, 1997, does not clearly state the Army Evaluation Center's responsibilities regarding the testing of system IA requirements.[21] To compensate, the Army Evaluation Center was

[19]Security testing is the examination and analysis of the safeguards, which are required to protect an information technology system, to determine the security posture of that system.

[20]The April 2002 and the June 2001 versions of DoD Regulation 5000.2-R have these same requirements as the DoD Guidebook.

[21]Army Regulation 25-1, "Army Information Management," May 31, 2002; also did not address the testers roles and responsibilities regarding information management.

using the procedures in the Director, Operational Test and Evaluation policy memorandum to determine whether DITSCAP testing of system IA requirements was sufficient or whether the system required additional IA testing during operational testing. On May 30, 2003, the Army Test and Evaluation Management Agency issued an update to Army Pamphlet 73-1. The IA section of the update states that the system evaluator must ensure that software is evaluated, independently tested, and verified to ensure it meets the minimum standards for security and reliability prior to release for operation. The Army Test and Evaluation Command was incorporating the guidance from the Director, Operational Test and Evaluation policy memorandum into an Army Evaluation Center handbook.

System Evaluation Reports. Of the 41 Army programs surveyed, we identified 5 programs where the Army Evaluation Center used Army Operational Test Command results from tests conducted in 2002 to prepare SERs. For three of the five SERs, the Army Evaluation Center stated in the applicable SERs that DITSCAP test data were not available to the evaluators to use as a data source for their IA evaluations. For the remaining two SERs, the Army Evaluation Center used DITSCAP test data in its IA evaluations.

The Army Evaluation Center also identified two additional SERs that resulted from 2002 test results for systems other than the 41 Army programs that we surveyed. DITSCAP test data was not available to the Army Evaluation Center in preparing those IA evaluations. The Army Evaluation Center attributed the nonavailability of DITSCAP test data to the need for an Army requirement for the SSAA signatories, including the applicable program managers, to coordinate with the Army Test and Evaluation Command throughout the acquisition cycle for Army systems subject to the DITSCAP. As a result, the Army Test and Evaluation Command did not always have the DITSCAP test results for use in system evaluations to advise the decision review principals and milestone decision authority on the adequacy of testing; the system's effectiveness, suitability, and survivability; as well as recommendations for future test and evaluation and system improvements.

Effect of the Availability of IA Testing Results

Because Army testers did not conduct IA testing and evaluation before system production decisions, milestone decision authorities did not have assurance that systems developed satisfied the IA requirements of availability, integrity, authenticity, confidentiality, and nonrepudiation of information to meet warfighter requirements as envisioned in the Quadrennial Defense Review and Joint Vision 2020.

Management Comments on the Finding

Although not required to comment, the Director, Operational Test and Evaluation agreed with the finding. For the complete text of the Director's comments, see the Management Comments section of the report.

Recommendations, Management Comments, and Audit Response

C.1. We recommend that the Assistant Secretary of the Army (Acquisition, Logistics, and Technology), in coordination with the Director, Test and Evaluation Management Agency, update Army Regulation 70-1, "Army Acquisition Policy," December 15, 1997, to:

a. Require the Army Training and Doctrine Command to coordinate with the Army Test and Evaluation Command:

(1) When developing testable information assurance requirements for inclusion in operational requirements documents for new Army acquisition programs with interoperability and supportability requirements.

(2) When updating existing operational requirements documents for Army acquisition programs with interoperability and supportability requirements to ensure that those documents have testable information assurance requirements.

Acting Deputy for Systems Management, Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) Comments. The Acting Deputy concurred, stating that the Army is updating Army Regulation 70-1 and expects to publish it in late November 2003. Further, he stated that the Army will not repeat requirements in the DoD 5000 series or Army Regulation 73-1 in the updated regulation. The Acting Deputy also stated that this approach meets the intent of the recommendations in the report to ensure that:

- program managers develop C4I support plans,
- program managers achieve joint interoperability testing and certifications for their systems,
- testable IA requirements are clearly identified, and
- the DITSCAP identifies the responsibilities of the combat developers.

For the complete text of the Acting Deputy's comments, see the Management Comments section of the report.

Principal Director for Enterprise Integration Comments. Although not required to comment, the Principal Director disagreed with the recommendation, stating that we should revise the recommendation because including testable IA requirements in new or updated ORDs would neither eliminate duplicative testing nor meet DITSCAP requirements. The Principal Director also stated that, to meet

DITSCAP requirements, the designated approving authority, the certification authority, the program manager, and the user representative must:

- determine the applicable governing national, DoD, and Army security requirements, network connection rules, and configuration management requirements for a system; and

- agree on the security and certification level for the system based on those requirements.

In addition, he stated that those requirements are documented in an applicable Requirements Traceability Matrix, which is a DITSCAP-required appendix to the associated SSAA. The Principal Director also stated that the system must be tested against those requirements in the Requirements Traceability Matrix, not those in the ORD. Further, he stated that the results of the certification tests should be available to the designated approving authority, the program manager, and the user representative before the system undergoes operational testing. The Principal Director also stated that the certification authority, who must be independent from the program manager, is one of the signatories of the SSAA. For the complete text of the Principal Director's comments, see the Management Comments section of the report.

Audit Response. The Principal Director's comments conflict with DoD guidance. Including testable IA requirements in new or updated ORDs should minimize duplicative testing and meet DITSCAP requirements as stipulated in DoD Instruction 5000.2 and Director, Operational Test and Evaluation memorandum, "Policy for Operational Test and Evaluation of Information Assurance." In addition, the DoD Guidebook states that IA testing should be conducted on information systems to ensure that planned and implemented security measures satisfy ORD and SSAA requirements when the system is installed and operated in its intended environment. Further, DoD Manual 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 31, 2000, states that the SSAA is to be tailored to meet the characteristics of the information system, operational requirements, security policy, and prudent risk management. Tailoring permits the DITSCAP to remain responsive to operational requirements and priorities.

Director, Operational Test and Evaluation Comments. Although not required to comment, the Director agreed with the recommendation. For the complete text of the Director's comments, see the Management Comments section of the report.

b. Identify roles and responsibilities of combat developers in the DoD Information Technology Security Certification and Accreditation Process.

Acting Deputy for Systems Management Comments. The Acting Deputy concurred, stating that the Army is updating Army Regulation 70-1 to ensure that the DITSCAP identifies the responsibilities of the combat developers.

Principal Director for Enterprise Integration Comments. Although not required to comment, the Principal Director agreed with the recommendation,

stating that the Army is replacing Army Regulation 380-19, "Information Systems Security," February 27, 1998, with Army Regulation 25-IA that will define DITSCAP roles and responsibilities for the designated approving authority, the program manager, and the certification authority. Further, he agreed with designating TRADOC as the user representative in Army Regulation 70-1.

Director, Operational Test and Evaluation Comments. Although not required to comment, the Director agreed with the recommendation.

c. Require the system security authorization agreement signatories to coordinate with the Army Test and Evaluation Command throughout the acquisition cycle for Army systems subject to the DoD Information Technology Security Certification and Accreditation Process.

Acting Deputy for Systems Management Comments. The Acting Deputy concurred, stating that the Army is updating Army Regulation 70-1 to ensure that testable IA requirements are clearly identified.

Principal Director for Enterprise Integration Comments. Although not required to comment, the Principal Director stated that the report implies that the Army Test and Evaluation Command should act in the capacity of the DITSCAP certification authority. Further, he stated that, in the long term, the recommendation has merit; however, for the Army Test and Evaluation Command to perform the DITSCAP certification tests, the Command must employ personnel who can meet or exceed the qualifications and standards of the National Security Telecommunications and Information Systems Security Instruction 4015 and the Army Regulation 380-53, "Information Systems Security Monitoring," April 29, 1998.

Audit Response. The intent of the recommendation was not to have the Army Test and Evaluation Command act as the DITSCAP certification authority, but instead, to have SSAA signatories coordinate with the Army Test and Evaluation Command so that the Command would have DITSCAP test results in time for inclusion in their SERs.

Director, Operational Test and Evaluation Comments. Although not required to comment, the Director agreed with the recommendation.

C.2. We recommend that the Army Chief Information Officer validate all warfighting requirements through the review of appropriate requirements documents to ensure that a system security authorization agreement has been prepared for Army systems subject to the DoD Information Technology Security Certification and Accreditation Process, in accordance with Army Regulation 25-1, "Army Information Management," May 31, 2002.

Principal Director for Enterprise Integrations Comments. The Principal Director, responding for the Army Chief Information Officer, concurred, stating that Army Regulation 380-19, which is being replaced with Army Regulation 25-IA, is the governing regulation for the certification and accreditation of Army systems. Further, he stated that the Army Information Assurance Directorate validates security requirements for Army systems by

conducting reviews of capability development documents (formerly called ORDs) and SSAAs. The Principal Director also stated that the Army Information Technology Security Registry is being enlarged to include the security parameters of Army information technology systems required by the Federal Information Security Management Act. In addition, he stated that the Army Information Technology Security Registry will track the accreditation status of information technology systems as well as other security-relevant parameters. The Principal Director stated that the Information Assurance Directorate assesses IA strategies, required by Section 8088 of the Clinger Cohen Act, which support system milestone decisions.

Director, Operational Test and Evaluation Comments. Although not required to comment, the Director agreed with the recommendation.

Appendix A. Scope and Methodology

We reviewed documentation dated from March 1994 to May 2003. To accomplish the audit objective, we reviewed:

- the Army's efforts to implement interoperability and information assurance requirements during the acquisition process;
- requirements documentation for interoperability and information assurance requirements;
- the controls over the Joint Staff (J-6) interoperability certification process and the Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool; and
- applicable criteria.

We also contacted the staffs of the Chairman of the Joint Chiefs of Staff; the Assistant Secretary of Defense (Networks and Information Integration); the Assistant Secretary of the Army (Acquisition, Logistics, and Technology); the Defense Information Systems Agency; the Army Training and Doctrine Command; the Office of the Army Chief Information Officer; the Army Deputy Chief of Staff for Operations and Plans; the Army Test and Evaluation Management Agency; the Army Test and Evaluation Command.

Further, we judgmentally selected 41 new or modified Army acquisition programs with research and development funding that interface with other systems to:

- obtain the program managers' perspectives on interoperability and IA requirements;
- review ORDs, C4I Support Plans, TEMPs, and SSAAs;
- review the status of interoperability testing by the Joint Interoperability Test Command; and
- determine the stage of each program in the Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool for Joint Staff (J-6) interoperability certification.

We performed this audit from July 2002 through June 2003 in accordance with generally accepted government auditing standards. We did not review the management control program because the audit focused on interoperability and IA requirements and review processes; therefore, our scope was limited to those specific requirements and processes.

Use of Computer-Processed Data. We did not rely on computer-processed data to perform this audit.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the DoD weapon systems acquisition high-risk area.

Prior Coverage

During the last 5 years, the General Accounting Office, the Inspector General of the DoD, and the Defense Science Board have issued five reports addressing interoperability and IA requirements for Defense systems. Unrestricted General Accounting Office and Inspector General of the Department of Defense reports can be accessed at http://www.gao.gov and http://www.dodig.osd.mil/audit/reports, respectively.

General Accounting Office (GAO)

GAO Report No. NSIAD-98-73, "Joint Military Operations: Weakness in DoD's Process for Certifying C4I Systems' Interoperability," March 1998

Inspector General of the Department of Defense (IG DoD)

IG DoD Report No. D-2003-011, "Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems," October 17, 2002

IG DoD Report No. D-2001-176, "Survey of Acquisition Manager Experience using the DoD Joint Technical Architecture in the Acquisition Process," August 22, 2001

IG DoD Report No. D-2001-121, "Use of the DoD Joint Technical Architecture in the Acquisition Process," May 14, 2001

Defense Science Board

Defense Science Board Task Force, "Protecting the Homeland, Report of the Defense Science Board Task Force on Defensive Information Operations, 2000 Summer Study, Volume II," March 2001

Appendix B. Glossary

Accreditation. Accreditation is the formal declaration by the designated approving authority that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Acquisition Category. An acquisition category is an attribute of an acquisition program that determines the program's level of review, decision authority, and applicable procedures. The acquisition categories consist of I, major Defense acquisition programs; IA, major automated information systems; II, major systems; III, programs not meeting the criteria for acquisition categories I, IA, or II; and IV, programs designated as such by the Army, Navy, and Marine Corps.

Advanced Concept Technology Demonstration. An advanced concept technology demonstration is used to determine the military utility of proven technology and to develop the concept of operations that will optimize effectiveness. Advanced concept technology demonstrations are not themselves acquisition programs, but are designed to provide a residual, usable capability upon completion, and possibly transition into acquisition programs. Funding is programmed to support the demonstration for up to 2 years in the field.

Architecture. An architecture is the structure of components, their interrelationships, and the principal guidelines governing their design and evolution over time.

Army Enterprise Infostructure-Transport. The Army Enterprise Infostructure-Transport will establish one Army network to support all Army applications. The Infostructure establishes a network-centric environment that enables seamless communications, anytime, anywhere. The Army Enterprise Infostructure-Transport concept is the approach that the Army will use to outline how each system will interface within the GIG to achieve joint interoperability.

Capstone Requirements Document. A capstone requirements document is a document that contains capabilities-based requirements that facilitate the development of individual ORDs by providing a common framework and operational concept to guide their development. It is an oversight tool containing overarching requirements for a system-of-systems or family-of-systems.

Certification Authority. Certification authority is the official responsible for performing the comprehensive evaluation of the technical and nontechnical security features of an information technology system and other safeguards to determine the extent to which a particular design and implementation meet a set of specified security requirements.

Combat Developer. A combat developer is the command or agency that formulates and documents operational concepts, doctrine, organizations, and or materiel requirements (mission need statements and operational requirements documents) for assigned mission areas and functions. A combat developer serves

as the user representative during acquisitions for their approved materiel requirements as well as doctrine and organization developments.

Command, Control, Communications, Computers, and Intelligence Support Plan. A C4I support plan describes system dependencies and interfaces in sufficient detail to enable program managers and operational testers to test interoperability key performance parameters derived from information exchange requirements.

Command, Control, Communications, Computers, and Intelligence Surveillance and Reconnaissance Architecture Framework. The C4I surveillance and reconnaissance architecture framework provides rules, guidance, and product descriptions for developing and presenting different architectural views of a given system to ensure a common denominator for understanding, comparing, and integrating architectures across DoD.

Critical Operational Issue. A critical operational issue is a key operational effectiveness issue or operational suitability issue that must be examined in the operational test and evaluation to determine the system's capability to perform its mission.

Defense Information Infrastructure. Defense information infrastructure is the seamless web of communications networks, computers, software, databases, applications, data, security services, and other capabilities that meets the information processing and transport needs of DoD users in peace and in all crises, conflict, humanitarian support, and wartime roles.

Defense Information Infrastructure Common Operating Environment. The Defense Information Infrastructure Common Operating Environment is a mission application independent architecture comprising reusable software and a set of guidelines based on the Joint Technical Architecture.

Designated Approving Authority. The designated approving authority is an official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The term designated approving authority is synonymous with designated accrediting authority and delegated accrediting authority.

Developmental Test and Evaluation. Developmental test and evaluation is any engineering type of test used to verify the status of technical progress, verify that design risks are minimized, substantiate achievement of contract technical performance, and certify readiness for initial operational testing. Generally, those tests are instrumented and measured by engineers, technicians, or soldier operator-maintainer test personnel in a controlled environment to facilitate failure analysis.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The DITSCAP is the standard DoD process for identifying information security requirements, providing security solutions, and managing information system security activities.

DITSCAP Certification. DITSCAP certification is the comprehensive evaluation of the technical and nontechnical security features of an information technology system and other safeguards made in support of the accreditation process to establish the extent that a particular design and implementation meets a set of specified security requirements.

Enterprise Architecture. An enterprise architecture is the explicit description and documentation of the current and desired relationships among business and management processes and information technology. The enterprise architecture describes the "current architecture" and "target architecture" to include the rules, standards, and system life cycle information to optimize and maintain the environment that the agency wishes to create and maintain by managing its IT portfolio.

Evolutionary Acquisition. Evolutionary acquisition is an acquisition approach in which the ultimate capability delivered to the user is divided into two or more blocks. Block 1 provides the initial deployment capability, a usable increment of capability called for in the ORD. The remaining capability is provided in subsequent blocks. The allocation of requirements to be achieved in each remaining block may be known and defined at the beginning of the block program, or may be defined for particular blocks "lead time away" from the start of work beginning on a block, based on the user's increased understanding of the delivered capability, the evolving threat, or available technology.

Global Information Grid. The Global Information Grid provides the foundation for network-centric warfare, information superiority, decision superiority, and ultimately, full spectrum dominance. The GIG includes any system, equipment software, or service that transmits information to, receives information from, routes information among or interchanges information among other equipment, software, and services. Non-GIG information technology is stand-alone, self-contained, or embedded information technology that is not and will not be connected to the enterprise network.

Information Assurance. Information assurance is information operations that measure, protect, and defend the information and information systems by ensuring their availability, integrity, confidentiality, authentication and nonrepudiation. Information assurance provides for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Exchange Requirements. Information exchange requirements characterize the information exchanges to be performed by a proposed system and identify who exchanges what information with whom, why the information is necessary, and how the users will employ that information.

Information Management. Information management consists of activities required to coordinate, plan, organize, analyze, integrate, evaluate, and control information resources effectively.

Information System. An information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. An

information system includes automated information system applications, enclaves, outsourced information-technology-based processes, and platform information technology interconnections.

Information Technology. Information technology is the hardware, firmware, and software used as part of the information system to perform DoD information functions. Information technology includes computers, telecommunications, automated information systems, automatic data processing equipment, and any assembly of computer hardware, software, and firmware configured to collect, create, communicate, compute, disseminate, process, store, and control data or information.

Interoperability. Interoperability is the ability of systems, units, or forces to provide services to or accept services from other systems, units, or forces and to use the services so exchanged to operate effectively together.

Interoperability Certification. Certification as it applies to interoperability is a formal statement of adequacy provided by a responsible agency (usually Joint Staff) attesting that a system has met its interoperability and supportability requirements.

Joint Mission Area. A joint mission area is a functional group of joint tasks and activities that share a common purpose and facilitate joint force operations.

Joint Operational Architecture. A joint operational architecture describes tasks and activities, operational elements, and information flows required to accomplish or support military operations; defines types of information exchanged, frequency of exchange, which tasks and activities are supported by information exchanges, and nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.

Joint Requirements Oversight Council. The Joint Requirements Oversight Council assists the Chairman of the Joint Chiefs of Staff in identifying and assessing the priority of joint military requirements (including existing systems and equipment) to meet the national military strategy. The council, chaired by the Vice Chairman of the Joint Chiefs of Staff and consisting of all the Vice Chiefs of the Military Departments including the Assistant Commandant of the Marine Corps, directly supports the Defense Acquisition Board through review, validation, and approval of key cost, schedule, and performance parameters at the start of the acquisition process, before each milestone review, and as requested by the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Joint Technical Architecture. The Joint Technical Architecture is a common set of mandatory information technology standards, which are primarily interface standards and guidelines to be used by all emerging systems and systems upgrades, including advanced concept technology demonstrations. The Joint0 Technical Architecture can be used to establish a system's technical architecture, and is applicable to all C4I and automated information systems and the interfaces of other key assets, such as weapon systems and sensors, with C4I systems.

Key Performance Parameters. Key performance parameters are a critical subset of the performance parameters found in the ORD. Each key performance parameter has a threshold and an objective value. Key performance parameters represent those capabilities or characteristics so significant that failure to meet the threshold value of performance can be cause for the concept or system selected to be reevaluated or the program to be reassessed or terminated.

Mission Need Statement. A mission need statement is a formatted non-system-specific statement containing operational capability needs that is written in broad operational terms.

National Security System. A national security system is any telecommunication or information system operated by the U.S. Government, whose function, operation, or use involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon system, or is critical to the direct fulfillment of military or intelligence missions.

Network-Centric Warfare. Network-centric warfare[22] allows a warfighting force to achieve improved information positions in the form of common operational pictures that provide the basis for shared situational awareness and knowledge, and a resulting increase in combat power.

Objective. The objective is the performance value that is desired by the user and which the program manager is attempting to obtain. The objective value represents an operationally meaningful, time critical, and cost effective increment above the performance threshold for each program parameter.

Objective Force. The Objective Force will be a system of systems, networked internally and externally through a responsive, reliable, mobile, non-line-of-sight, and commander-and-executive-centric command and control capability. The Objective Force will leverage joint/interagency reachback and Army direct downlink capabilities for intelligence, personnel and force planning, administration, technical engineering, information operations and logistical support.

Operational Architecture View. The operational architecture view is a description of the tasks and activities, operational elements, and information flows required to accomplish or support a military operation.

Operational Effectiveness. Operational effectiveness is the overall degree of mission accomplishment of a system when representative personnel use the system in the environment planned or expected for operational employment of the system, considering organization, doctrine, tactics, survivability, vulnerability, and threat.

[22]An in-depth discussion of network-centric warfare is provided in the book, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised), by David S. Alberts, John J. Garstka, and Frederick P. Stein, C^4I Surveillance and Reconnaissance Cooperative Research Program, August 1999.

Operational Requirements Document. The operational requirements document states the user's objectives and minimum acceptable requirements for the operational performance of a proposed concept or system.

Operational Suitability. Operational suitability is the degree to which a system can be placed satisfactorily in field use with consideration being given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistic supportability, natural environmental effects, documentation, and training requirements.

Operational Test and Evaluation. Operational test and evaluation is field testing, under realistic conditions, of any item or component of weapons, equipment, or munitions to determine their effectiveness and suitability for use in combat by typical military users and the evaluation of the results of such tests.

Penetration Testing. Penetration testing assesses a system's ability to withstand intentional attempts to circumvent system security features by exploiting technical security vulnerabilities. Penetration testing may include insider and outsider penetration attempts based on common vulnerabilities for the technology being used.

Program. A program is an acquisition funded by research, development, test and evaluation or procurement appropriations, or both, with the express objective of providing a new or improved capability in response to a stated mission need or deficiency.

Program Manager. Program manager refers to the acquisition organization's program manager during the system acquisition, the system manager during the operation of the system, or the maintenance organization's program manager when a system is undergoing a major change.

Risk. Risk is a combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse effect, and the severity of the resulting adverse effect.

Survivability. Survivability is the capability of a system to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission.

System. A system is the organization of hardware, software, materiel, facilities, personnel, data, and services needed to perform a designated function with specified results, such as the gathering of specified data, its processing, and delivery to users.

System Evaluation Plan (SEP). The SEP documents the integrated test and evaluation strategy, which the testers and evaluators use throughout the system acquisition life cycle. The SEP:

- addresses system critical operational issues and criteria, critical technical parameters, and additional evaluation focus areas;

- identifies data needs and sources, and the approach to be used to evaluate the system;
- specifies the analytical plan; and
- identifies program constraints.

The SEP details the evaluator's planned actions for the evaluation of the system and is prepared and updated by the system evaluator.

System Evaluation Report (SER). The SER documents independent evaluation findings and recommendations on system operational effectiveness, suitability, and survivability. The SER addresses and answers the critical operational issues and additional evaluation focus areas in the SEP. The system evaluator produces a SER to advise the decision review principals and milestone decision authority concerning the adequacy of testing, the system's effectiveness, suitability, and survivability, as well as recommendations for future test and evaluation and system improvements. The SER enables the milestone decision authority to make an informed decision on system production.

System Evaluator. The system evaluator is an Army command or agency that assesses program effectiveness, suitability, and survivability (or progress towards achieving these) during each phase in the system's life cycle. Further, the system evaluator is responsible for planning, conducting, and reporting the system evaluation or assessment.

System-of-Systems. System-of-systems, also known as a family-of-systems, is several independent programs which, when integrated, form a system to meet the needs of a broad mission area such as missile defense. The performance of the individual component programs making up the system-of-systems is specified in the respective program ORDs; the overarching requirements for the system-of-systems are contained in a CRD.

System Security Authorization Agreement. The system security authorization agreement is a formal agreement among the designated approving authority, the certification authority, the information technology system user representative, and the program manager. The agreement is used throughout the entire DITSCAP to guide actions, document decisions, specify information technology security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

System Security Authorization Agreement Signatories. The system security authorization agreement signatories include the information technology system program manager, the designated approving authority, the certification authority, and the user representative.

Technical Architecture View. A technical architecture view is a minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set or requirements.

Test and Evaluation Master Plan. The test and evaluation master plan documents the overall structure and objectives of the test and evaluation program. It provides a framework within which to generate detailed test and evaluation plans and it documents schedule and resource implications associated with the test and evaluation program. The test and evaluation master plan identifies the necessary developmental test and evaluation, operational test and evaluation, and live-fire test and evaluation activities. Further, the test and evaluation master plan relates program schedule, test management strategy and structure, and required resources to critical operational issues, critical technical parameters, objectives and thresholds documented in the operational requirements document, evaluation criteria, and milestone decision points.

Test Integration Working Group. The Test Integration Working Group facilitates the integration of test requirements through close coordination among the materiel developer, combat developer, logistician, and developmental and operational testers to minimize development time and cost and preclude duplication between developmental and operational testing.

Threshold. Threshold is the minimum acceptable value that, in the user's judgment, is necessary to satisfy the need. If threshold values are not achieved, program performance is seriously degraded, the program may be too costly, or the program may no longer be timely.

User Representative. The user representative is the liaison for the user or the user community, particularly during the initial development of a system. The user representative is the individual or organization that represents the user community in the specification, acquisition and maintenance of information technology system. The user representative defines the system mission and functionality and is responsible for ensuring that the user's interests are maintained throughout system development, modification, integration, acquisition, and deployment.

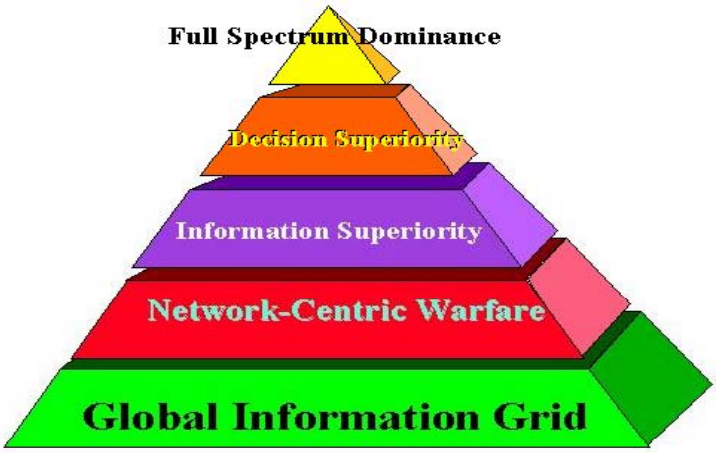
Validation. Validation is an authoritative act or process of supporting or corroborating whether information technology and NS system interoperability and supportability requirements are appropriate.

Verification. Verification is the act of establishing whether information technology and NS system interoperability requirements are accurate, measurable, supportable, and adequately reflected in a system or family of systems' acquisition strategy, test and evaluation plan, or in non-materiel or non-traditional acquisition information technology and NS system interoperability plans.

Vulnerability. Vulnerability is the characteristics of a system that cause it to suffer a definite loss or reduction of capability to perform its designated mission as a result of having been subjected to a certain level of effects in a man-made hostile environment.

Appendix C. Global Information Grid

Global Information Grid. The GIG provides the foundation for network-centric warfare, information superiority, decision superiority, and ultimately full spectrum dominance as depicted in the figure below.



Foundation for Achieving Full Spectrum Dominance[23]

The concept of the GIG evolved from concerns about the interoperability and end-to-end integration of automated information systems. Issues such as streamlined management and improved information infrastructure investment also contributed to the heightened interest in a GIG. However, the real demand for a GIG originates from the requirement for information and decision superiority to achieve full spectrum dominance, as expressed in Joint Vision 2020. The ability to achieve shared situational awareness and knowledge among all elements of a joint force, including allied and coalition partners, is increasingly viewed as a cornerstone to transform future warfighting capabilities.

Network-Centric Warfare. The GIG capstone requirements document states that network-centric warfare allows a warfighting force to achieve improved information positions in the form of common operational pictures that provide the basis for shared situational awareness and knowledge, and a resulting increase in combat power.

Information Superiority. Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority is achieved in a noncombat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives. Information superiority provides the joint force with a competitive

[23]Figure obtained from the GIG Capstone Requirements Document, August 30, 2001.

advantage only when it is effectively translated into superior knowledge and decisions. The joint force must be able to take advantage of superior information converted to superior knowledge to achieve "decision superiority."

Decision Superiority. Decision superiority is to arrive at better decisions and implement them faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission. Decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation, relevant training and experience, and the proper command and control mechanisms and tools are equally necessary.

Full Spectrum Dominance. The transformation of the joint force to reach full spectrum dominance rests upon information superiority as a key enabler and our capacity for innovation. The label full spectrum dominance implies that U.S. Forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific situations and with access to and freedom to operate in all domains: space, sea, land, air, and information. Additionally, given the global nature of our interests and obligations, the United States must maintain its overseas presence forces and the ability to rapidly project power worldwide in order to achieve full spectrum dominance.

Appendix D. Army Interoperability and Information Assurance Survey Results

Survey Question	Survey Answers	Number of Program Managers Responded
1. What acquisition category is your program?	a. Acquisition Category I AM or Acquisition Category I AC	0
	b. Acquisition Category I D or Acquisition Category I	9
	c. Acquisition Category II	13
	d. Acquisition Category III	14
	e. Other	4
2. What type of system is your program?	a. NS system	14
	b. Information technology system (that is not an NS system)	5
	c. Weapon system	8
	d. Automated information system	8
	e. None of the above	5
3. What is the last milestone your program completed?	a. Pre-acquisition (e.g., science and technology, concept development, demonstration)	1
	b. Milestone A (or 0)	3
	c. Milestone B (or II or system development and demonstration)	13
	d. Milestone C (or III or operational system development)	4
	e. Beyond Milestone C (or full-rate production)	14
	f. Other	6
4. Which joint mission area does your program support? Select the appropriate answer based on the Chairman of the Joint Chiefs of Staff Memorandum (CM-1014-00), "Joint Mission Areas to Organize the Joint Operational Architectures."	a. Dominant maneuver	12
	b. Deployment redeployment	3
	c. Precision engagement	7
	d. Strategic deterrence	0
	e. Overseas presence and force projection	7
	f. Special operations	1
	g. Joint command and control	11
	h. Information superiority	14
	i. Focused logistics	3
	j. Full dimensional protection	7
	k. Multinational operations/ interagency coordination	4
	l. Other	14

Survey Question	Survey Answers	Number of Program Managers Responded
5. For information technology or NS systems, the ORD must include interoperability requirements, thus requiring an interoperability key performance parameter. These systems must also have related elements of IA. In this respect, do you think IA is a subcomponent of interoperability?	a. Yes	31
	b. No	8
	c. Unsure	2
6. Should IA requirements be tested in addition to interoperability requirements?	a. Yes	34
	b. No	3
	c. Unsure	3
7. Has the Joint Staff J-6 certified your program's ORD for interoperability requirements?	a. Yes	17
	b. No, the ORD has not been through the process yet.	8
	c. No, the ORD went through the process but was not certified	1
	d. In process	8
	e. Unsure	7
8. Is your program part of the GIG asset inventory?	a. Yes	17
	b. No	11
	c. Unsure	12
9. How is your program compatible with the GIG? Select all that apply.	a. Uses current defense information switched network services	12
	b. Uses approved allocated frequency plans	17
	c. Uses approved cryptology	18
	d. Meets appropriate standards (e.g., defense information infrastructure common operating environment compliance)	29
	e. None of the above	3
	f. Other	5
	g. Unsure	1

Survey Question	Survey Answers	Number of Program Managers Responded
10. Which Army oversight entity(ies) or command(s) ensures that your Acquisition Category I AM, I AC, I D, or I C operates with other Defense agency and Military Department acquisition programs as envisioned by the warfighter.	a. Program executive officer/milestone decision authority	16
	b. Army Deputy Chief of Staff for Programs	7
	c. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)	10
	d. Army Test Command	9
	e. TRADOC	12
	f. Deputy of Information Systems for C4I	10
	g. Army Materiel Command	1
	h. Army Intelligence and Security Command	3
	i. Joint Staff J-6	6
	j. U.S. Joint Forces Command (J-6)	3
	k. Other	23
11. Which Army oversight entity(ies) or command(s) ensures that your Acquisition Category II or below program operates with other Defense agency and Military Department acquisition programs as envisioned by the warfighter.	a. Program executive officer/milestone decision authority	29
	b. Army Deputy Chief of Staff for Programs	5
	c. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)	10
	d. Army Test Command	3
	e. TRADOC	11
	f. Deputy of Information Systems for C4I	10
	g. Army Materiel Command	6
	h. Army Intelligence and Security Command	1
	i. Other	8
12. Of the following documentation normally provided to the milestone decision authority at Milestone B, which documents fully describe interoperability requirements and strategies? Select all that apply.	a. ORD	31
	b. CRD	8
	c. C4I support plan	21
	d. TEMP	24
	e. Developmental test results	12
	f. Operational test results	11
	g. SEP	11
	h. Event design plan	9
	i. Operational architecture view	18
	j. Systems architecture view	16
	k. Technical architecture view	15
	l. Security plans	13
	m. Other	9
	n. None	2

Survey Question	Survey Answers	Number of Program Managers Responded
13. Of the following documentation normally provided to the milestone decision authority at Milestone C, which documents fully describe interoperability requirements and strategies? Select all that apply.	a. ORD	32
	b. CRD	8
	c. C4I support plan	23
	d. TEMP	29
	e. Developmental test results	20
	f. Operational test results	23
	g. SEP	18
	h. Event design plan	9
	i. Operational architecture view	16
	j. Systems architecture view	16
	k. Technical architecture view	17
	l. Security plans	13
	m. Other	6
	n. None	0
14. Of the following documentation normally provided to the milestone decision authority at Milestone B, which documents fully describe IA requirements and strategies? Select all that apply.	a. ORD	19
	b. CRD	4
	c. C4I support plan	15
	d. TEMP	13
	e. SSAA	20
	f. Developmental test results	5
	g. Operational test results	7
	h. SEP	7
	i. Event design plan	3
	j. Operational architecture view	8
	k. Systems architecture view	6
	l. Technical architecture view	6
	m. Security plans	11
	n. Other	7
	o. None	2
15. Of the following documentation normally provided to the milestone decision authority at Milestone C, which documents fully describe IA requirements and strategies? Select all that apply.	a. ORD	22
	b. CRD	5
	c. C4I support plan	18
	d. TEMP	19
	e. SSAA	29
	f. Developmental test results	12
	g. Operational test results	13
	h. System evaluation plan	12
	i. Event design plan	5
	j. Operational architecture view	10
	k. Systems architecture view	10
	l. Technical architecture view	8
	m. Security plans	16
	n. Other	7
	o. None	1

Survey Question	Survey Answers	Number of Program Managers Responded
16. The inclusion of IA requirements in an ORD would benefit from the addition of high-level information exchange requirements. (See Chairman of the Joint Chiefs of Staff Instruction 3170.01B, "Requirements Generation System.")	a. I agree b. I disagree c. I am unsure	31 6 2
17. The ORD must define information exchange requirements for information technology and NS system acquisition programs.	a. I agree b. I disagree c. I am unsure	33 5 1
18. IA should be a key performance parameter in my acquisition program that must exchange data external to the information technology and NS system, or weapon system's host platform.	a. I agree b. I disagree c. I am unsure	22 12 2
19. My acquisition program will include the following IA security techniques or technologies before production. Select all that apply.	a. Public key infrastructure b. Firewalls c. Smart cards d. Passwords e. Encryption/decryption f. Physical security g. Frequency hopping h. Restoration of capability i. None of the above j. Other ____	7 17 3 34 27 31 16 20 0 8
20. My acquisition program will include the following IA security techniques or technologies after production. Select all that apply.	a. Public key infrastructure b. Firewalls c. Smart cards d. Passwords e. Encryption/decryption f. Physical security g. Frequency hopping h. None of the above i. Other	9 16 6 31 27 30 17 2 10
21. List all IA products that are commercial off-the-shelf products related and/or integrated into your acquisition program.	The program offices identified different commercial off-the-shelf products. A list of the products identified is available upon request.	32

Survey Question	Survey Answers	Number of Program Managers Responded
22. Are all the products listed in question 21 certified for IA by the National Security Agency?	a. Yes b. No c. Unsure	10 14 5
23. Do you plan to have all products listed in question 21 certified for IA by the National Security Agency? Answer if question 22 was No.	a. Yes b. No c. If no, why not?	6 12 11
24. Do fluctuations in funding and prioritization affect system development as it relates to interoperability requirements?	a. Yes b. No c. If so, how?	24 12 12
25. Is your program in compliance with the Clinger-Cohen Act?	a. Yes b. No c. If no, why not?	34 2 5
26. Do you believe the GIG currently addresses all IA requirements?	a. Yes b. No c. If no, what does it not address?	22 11 11

Appendix E. Army Programs Surveyed

1. Army Airborne Command and Control System
2. Advanced Field Artillery Tactical Data System Control System
3. Army Key Management System
4. Air and Missile Defense Planning Control Systems
5. All Source Analysis System
6. Aviation Combined Arms Tactical Trainer
7. Close Combat Tactical Trainer
8. Combat Service Support Control System
9. Defense Message System-Army
10. Enhanced Position Location Reporting System
11. Forward Area Air Defense Command, Control and Intelligence
12. Force XXI Battle Command Brigade-and-Below
13. Firefinder AN/TPQ-47
14. Global Combat Support System-Army
15. Global Positioning System Tactical Receivers
16. Guardrail/Common Sensor
17. Integrated Meteorological System
18. Integrated System Control
19. Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System
20. Joint Network Management System
21. Joint Service Lightweight Stand-off Chemical Agent Detector
22. Joint Surveillance Target Attack Radar System-Common Ground Sensor
23. Joint Tactical Ground Station
24. Joint Tactical Radio System
25. Land Warrior Integrated Soldier Fighting System
26. Medical Communications for Combat Casualty Care
27. Maneuver Control System
28. Medium Extended Air Defense System
29. Mobile Tower System
30. Movement Tracking System
31. Mounted Warrior Soldier System Cordless Communications
32. Phased Array Tracking to Intercept of Target (PATRIOT) Advanced Capability-3
33. Profiler
34. Prophet
35. Sentinel
36. Single Channel Ground and Airborne Radio System
37. Spitfire
38. Transformation Coordinators'-Automated Information for Movements System II
39. Tactical Exploitation System
40. Tactical Unmanned Aerial Vehicle
41. Warfighter Simulation System

Appendix F. Information Assurance Requirements Policy

DoD Directive 4630.5; DoD Directive 5000.1; DoD Directive 8500.1; DoD Instruction 5000.2; DoD Guidebook, "Interim Defense Acquisition Guidebook;"[24] Chairman of the Joint Chiefs of Staff Instruction 3170.01B; Army Regulation 70-1; and Army Regulation 73-1 discuss information assurance (IA) requirements generation and testing.

DoD Directive 4630.5. DoD Directive 4630.5 requires interoperability and supportability requirements to be balanced with the need for IA. Further, the Directive requires the DoD Components to ensure that program managers and testers prepare test and evaluation plans for all information technology and NS systems.

DoD Directive 5000.1. DoD Directive 5000.1 requires acquisition managers to address IA for all weapon, C4I surveillance and reconnaissance, and information technology programs that depend on external information sources or that provide information to other DoD systems.

DoD Directive 8500.1. DoD Directive 8500.1 requires the DoD Components to identify and include IA requirements in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems for which they have responsibility.

DoD Instruction 5000.2. DoD Instruction 5000.2 requires operational testers and evaluators to assess IA for all weapon, C4I surveillance and reconnaissance, and information programs that depend on external information sources or that provide information to other DoD systems.

DoD Instruction 8500.2. DoD Instruction 8500.2 requires the heads of DoD components to ensure that IA awareness, training, education, and professionalization are provided to all military and civilian personnel, including contractors, commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems in accordance with Deputy Secretary of Defense guidance. The Instruction also states that the heads of DoD components to provide for an IA monitoring and testing capability according to DoD Directive 4640.6. Further, the Instruction states that the IA Manager shall ensure that IA inspections, tests, and reviews are coordinated. In addition, the Instruction states that the ability to test and verify is an essential competency of the DoD IA program. Finally, the

[24]Formerly, DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," April 5, 2002. The Deputy Secretary's memorandum, "Defense Acquisition," October 30, 2002, and Attachment 2 to that memorandum reference a guidebook to accompany the interim guidance. The former DoD Regulation 5000.2-R will serve as the guidebook while the Defense Acquisition Policy Working Group creates a streamlined guidebook. The guidebook is not mandatory, but should be used for best practices, lessons learned, and expectations until replaced.

Instruction states that the IA objective condition is testable, IA compliance is measurable, and the activities required to achieve the IA Control are assignable and accountable.

DoD Guidebook. The Guidebook states that operational test and evaluation should determine:

- the operational effectiveness and suitability of a system under realistic operational conditions, including combat; and
- whether the system has satisfied thresholds and objectives in the approved ORD and the associated critical operational issues.

Joint Staff. Chairman of the Joint Chiefs of Staff Instruction 3170.01B requires all DoD systems that are used to enter, process, store, display, or transmit DoD information regardless of classification or sensitivity to address IA. Further, the Instruction requires the initial ORD to establish requirements describing the capabilities and characteristics of the proposed system. The Instruction also requires the requirements to be written in output-oriented and measurable terms in threshold and objective format with criteria and rationale for each.

Army Regulation 70-1. Army Regulation 70-1 requires the Army Training and Doctrine Command to develop and update ORDs.

Army Regulation 73-1. Army Regulation 73-1 states that a system's TEMP provides a map for integrated simulation, test and evaluation plans, schedules, and resource requirements necessary to accomplish the test and evaluation program. Further, the Regulation states that appropriate developmental testing assesses the achievement of critical technical parameters, identifies technological and design risks, determines readiness to proceed to the initial operational test, and provides data for system evaluations. In addition, the Regulation states that the initial operational test determines operational effectiveness, suitability, and the survivability of the system under realistic conditions.

Appendix G. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
    Director for Acquisition Initiatives
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Networks and Information Integration)
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff
    Director for Command, Control, Communications, and Computers Systems (J-6)
    Director for Force Structure, Resources, and Assessment (J-8)

Department of the Army

Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
Commander, Army Training and Doctrine Command
Commander, Army Test and Evaluation Command
Chief Information Officer, Department of the Army
Deputy Chief of Staff for Operations and Plans
Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Unified Command

Commander, U.S. Joint Forces Command

Other Defense Organizations

Director, Defense Information Systems Agency
    Commander, Joint Interoperability Test Command

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Director, Operational Test and Evaluation Comments

OPERATIONAL TEST AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

AUG 1 4 2003

MEMORANDUM FOR THE INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review of Draft Report on the Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems

My office has reviewed the subject draft report and I concur with your findings and recommendations.

Thomas P. Christie
Director

Secretary of the Army and Army Chief Information Officer Comments

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

22 September 2003

Office, Chief Information Officer / G-6
SAIS-EIG

MEMORANDUM FOR DOD INSPECTOR GENERAL, ATTN: MR. JOHN E. MELING, 400 ARMY NAVY DRIVE (ROOM 801) ARLINGTON, VA 22202-4704

SUBJECT: DODIG Draft Report – Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems (D2002AE-0187)

1. Reference DODIG Draft Report (D2002AE-0197), Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems.

2. The response to your recommendations contained in the draft report is provided at the enclosure.

3. The point of contact for this action is Ms. Angie Woodson, 703-602-9437, email woodsona@us.army.mil

Encl

GARY L. WINKLER
Principal Director for
Enterprise Intergration

RECOMMENDATIONS - DODIG REPORT D2002AE-0187:

RECOMMENDATION:
A. We recommend that the Secretary of the Army:

1. Issue and implement guidance to comply with DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002, which requires the Army to define how each Army system will interface within the Global Information Grid to achieve interoperability.

RESPONSE:
A.1. Concur with the recommendation. Army Regulations 25-1 (Army Information Management), and 70-1 (Army Acquisition Policy), are currently in revision and are addressing DoD Directive 8100.1 mandates. Mandates not adequately addressed will be incorporated into the next revision of these Army regulations. Moreover, the Army published its Army Knowledge Implementation Plan in September 2003 and, in its next revision, the Army will specifically address its plan to outline a policy to ensure its systems interface with the Global Information Grid.

RECOMMENDATION:
2. Expedite efforts to populate and maintain the Army's portion of the Global Information Grid asset inventory in accordance with DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002.

RESPONSE:
A.2. Concur with the recommendation. The Army has undertaken an aggressive effort to document its IT assets and expects to complete this effort by the end of 1st Qtr FY 04. By the end of 2nd Qtr FY 04 the Army will develop an enterprise management strategy to maintain visibility of these IT assets. The initial implementation of the enterprise management strategy will occur in 1st Qtr FY 05.

RECOMMENDATION:
3. Provide Army combat developers at the Army Training and Doctrine Command with training on how to implement the requirements of the Global Information Grid.

RESPONSE:
A.3. Concur with the recommendation. Using the strategy outlined in Army Knowledge Management goals, the Army will provide guidance to the Training and Doctrine command on how to develop training to implement the requirements of the Global Information Grid by the end of 4th Qtr FY 04.

RECOMMENDATIONS - DODIG REPORT D2002AE-0187 (CONTINUED):

RECOMMENDATION:
B. We recommend that the Army Deputy Chief of Staff for Operations and Plans, in coordination with the Army Chief Information Officer, update Army Regulation 70-1, "Army Acquisition Policy," December 15, 1997, and Army Regulation 71-9, "Materiel Requirements," April 30, 1997, to require that:

1. Combat developers identify interoperability and supportability requirements in requirements documents and update the requirements throughout the life of the systems, as necessary, in accordance with DOD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" January 11, 2002.

2. Program managers use command, control, communications, computers, and intelligence support plans to document interoperability and supportability requirements in accordance with DOD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 2, 2002.

3. Program managers obtain the Joint Staff J-6 certifications for interoperability in accordance with Chairman of the Joint Chiefs of Staff Instruction 6212.01B, "Interoperability and Supportability of National Security Systems, and Information Technology Systems, " May 8, 2000.

RESPONSE:
Concur with recommendations B.1-3. Army Regulations 70-1, Army Acquisition Policy, and 71-9, Materiel Requirements, are currently being updated by the ASA(AL&T) and G3 respectively. These recommendations will be incorporated into the revision. Publication of Army regulation 70-1 is expected in early FY04; Army regulation 71-9 is expected to be published mid-FY04. Please note, PMs should not be obtaining interoperability certifications (recommendation #3) unless by exception. Those should be done when the requirements/capabilities documentation is provided to the JS for review to include certification by J6 IAW CJCSI 6212.01B (soon to be "C"). That is part of the new CJCSI 3170.01C and was a requirement of the "B" version.

2

RECOMMENDATIONS - DODIG REPORT D2002AE-0187 (CONTINUED):

RECOMMENDATION:
C. 1. We recommend that the Assistant Secretary of the Army (Acquisition, Logistics, and Technology), in coordination with the Director, Test and Evaluation Management Agency, update Army Regulation 70-1, "Army Acquisition Policy," December 15, 1997, to:

a. Require the Army Training and Doctrine Command to Coordinate with the Army Test and Evaluation Command:

(1) When developing testable information assurance requirements for inclusion in operational requirements documents for new Army acquisition programs with interoperability and supportability requirements.

(2) When updating existing operational requirements documents for Army acquisition programs with interoperability and supportability requirements to ensure that those documents have testable information assurance requirements.

RESPONSE:
C.1.a. We recommend that the Inspector General revise their recommendation in C.1 of the report for the Assistant Secretary of the Army, Acquisition, Logistics, and Technology. The inclusion of testable Information Assurance requirements into new or updated operational requirements documents, while a commendable exercise will not eliminate duplicative testing nor meet DITSCAP requirements. To meet DITSCAP requirements, the Designated Approving Authority (DAA), the Certification Authority, the Program Manager, and the User Representative must determine the applicable governing National, DoD, and Army security requirements, network connection rules, and configuration management requirements, and reach an agreement on the security for the system and certification level based on these requirements. These requirements are documented in a Requirements Traceability Matrix (RTM), a DITSCAP required appendix of the Systems Security Authorization Agreement (SSAA). The Certification Authority, who must be independent from the Program Manager, is one of the signatories of the System Security Authorization Agreement. The system must be tested against those requirements documented in the RTM, not the ORD. The results of the certification tests should be available to the DAA, the Program Manager, and the User Representative <u>before</u> the system is sent for Operational Testing. While not stated as a straightforward recommendation within this report, it is implied that the Army Test and Evaluation Command should act in the capacity of the DITSCAP Certification Authority. In the long term, we believe this recommendation has merit. However, for the Army Test and Evaluation Command to perform the DITSCAP certification tests, they must employ personnel who can meet or exceed the qualifications and standards of the National Security Telecommunications and Information Systems Security

RECOMMENDATIONS - DODIG REPORT D2002AE-0187 (CONTINUED):

Instruction 4015 (see enclosure 1 for additional information) and in addition the specific qualifications stipulated in AR 380-53.

RECOMMENDATION:
C.1.b. Identify roles and responsibilities of combat developers in the DoD Information Technology Security Certification and Accreditation Process.

RESPONSE:
C.1.b. AR 380-19, and the pending replacement, AR 25-IA define DITSCAP roles and responsibilities for the DAA, the Program Manager, and the Certification Authority. We concur with naming, in AR 70-1, the TRADOC System Manager as the User Representative.

RECOMMENDATION:
C.1.c. Require the system security authorization agreement signatories to coordinated with the Army Test and Evaluation Command throughout acquisition cycle for Army systems subject to the DoD Information Technology Security Certification and Accreditation Process.

RESPONSE:
C.1.c. See C.1.a above.

RECOMMENDATION:
C.2. We recommend that the Army Chief Information Officer validate all warfighting requirements through the review of appropriate requirements documents to ensure that a systems security authorization agreement has been prepared for Army systems subject to the DoD Information Technology Security Certification and Accreditation Process, in accordance with Army Regulation 25-1, "Army Information Management," May 31, 2002.

RESPONSE:
C2. Concur with comment. Army Regulation AR 380-19, which is in the process of being replaced as AR 25-IA, is the governing regulation for the Certification and Accreditation of Army systems. Validation of security requirements for Army systems is accomplished by the Army Information Assurance Directorate through ongoing reviews of Capability Design Documents (formerly called Operational Requirements Documents) and System Security Authorization Agreements. The Army Information Technology Registry (AITR) is being enlarged to include security parameters of Army Information Technology (IT) Systems required by the Federal Information Security Management Act. The AITR will track the accreditation status of IT systems as well as other security-relevant parameters (attached). The Information Assurance Directorate assesses Information Assurance Strategies required by Section 8088 of the Clinger Cohen Act that support system milestone decisions.

FIELDS IN THE ARMY INFORMATION TECHNOLOGY REQUIREMENTS DATA BASE

Attachment

A: Component (e.g., Army)
B: System Component ID (e.g., DA00005)
C: Mission Critical (e.g., MC or ME)
D: System Acronym (e.g., AMS)
E: System Name
F: System Description
G: Functional Area (e.g., Logistics)
H: Secondary Functional Area
I: Tertiary Functional Area
J: Continuity Plan (Yes/No)
K: PM Name
L: PM Title
M: PM Organization
N: PM Commercial Phone Number
O: PM DSN Phone Number
P: PM E-Mail Address
Q: Last Updated (date)
R: Batch Date
S: ACAT (Acquisition Category)
T: Interfaces Identified (Yes/No)
U: BIN (Budget Initiative Number, if it exists, from the Information Technology Management Application (ITMA) Database
V: DoD IT Registry ID Number
W: Record Type (e.g., system, application, etc)
X: Life Cycle Phase (e.g., operations)
Y: Accreditation Status (e.g., IATO/Final)
Z: Accreditation Date
AA: Accreditation Vehicle (e.g., DITSCAP/DCID 6-3)
AB: Accreditation Documentation (Yes/No)
AC: SSAA Status (e.g., Phase I, II, III, or IV)
AD: Contingency Test (Yes/No)
AE: Access Controls (Yes/No)
AF: Admin Controls (Yes/No)
AG: Life Cycle Plan (Yes/No)
AH: Life Cycle Costs (Cost of Security Controls Integrated into Life Cycle Costs) (Yes/No)
AI: Maintenance Plan (Yes/No)
AJ: Risk Plan (Yes/No)
AK: Security Plan (Yes/No)
AL: CSIRT (Controls in place to recognize, report and handle incidents and share this information with appropriate organizations) (Yes/No)

FIELDS IN THE ARMY INFORMATION TECHNOLOGY REQUIREMENTS DATA BASE (CONTINUED)

Attachment

AM: Security Controls Test (Date Security Controls last tested)
AN: Virus Protection (Yes/No)
AO: GIG Compliant (To be completed by DoD)
AP: Waiver Expiration Date (To be completed by DoD)
AQ: Waiver Review Date (To be completed by DoD)
AR: DAA Name
AS: DAA Title
AT: DAA Organization
AU: DAA Phone
AV: DAA E-Mail

Assistant Secretary of the Army (Acquisition, Logistics, and Technology) Comments

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON DC 20310-0103

01 OCT 2003

SAAL-SI/CIO

MEMORANDUM FOR Department of Defense Inspector General

SUBJECT: Response to Draft DoD IG Report - Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems (D2002AE-0187).

The Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)) has reviewed the subject report, and concurs with comment on recommendations related to AR 70-1 and the acquisition process.

Army Regulation (AR) 70-1 "Army Acquisition Policy" is being rewritten and is expected to be published in late November. The construct of the revised regulation is complementary to both the DoD 5000 series documents on acquisition and AR 73-1 "Test and Evaluation Policy". In the update to AR 70-1 the Army has chosen not to repeat requirements set forth in the 5000 series or AR 73-1. This approach meets the spirit/intent of the recommendations made in the subject report with regard to:

(1) Ensuring program managers develop Command, Control, Communications, Computers, and Intelligence Support Plans (C4ISPs).

(2) Ensuring Program Managers achieve Joint Interoperability testing and certifications for their systems.

(3) Ensuring there is a clear identification of testable information assurance requirements and the identification of the responsibilities of the combat developer in the DoD Information Technology Security Certification and Accreditation Process.

My point of contact for this action is LTC Kathy Swacina, Deputy Chief Acquisition Oversight Division. Contact information for LTC Swacina, (703) 614-4287, e-mail: Kathleen.Swacina@saalt.army.mil.

S. M. Cannon

S. MICHAEL CANNON
Colonel (Promotable), AR
Acting Deputy for Systems Management

Team Members

The Acquisition Management Directorate, Office of the Deputy Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

John E. Meling
Jack D. Snider
Suellen R. Brittingham
Kevin W. Klein
Kelly R. McMaster
Jessica M. Ullrey
Jacqueline N. Pugh